Quest™

Foglight® Hybrid Cloud Manager for AWS 6.0.0

User and Administration Guide

their respective owners.

Legend

WARNING: **A WARNING icon indicates a potential for property damage, personal injury, or death.**

CAUTION: **A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Foglight Hybrid Cloud Manager for AWS User and Administration Guide
Updated - May 2021
Software Version - 6.0.0

Contents

1

Using Foglight Hybrid Cloud Manager for AWS

Foglight® Hybrid Cloud Manager for AWS is provided to meet the demand for monitoring the hybrid strategy, protecting the business, reducing tasks for users who want to monitor Infrastructure as a Service (IaaS) assets.

Foglight Hybrid Cloud Manager for AWS offers the ability to enable IaaS monitoring across Foglight performance agents and to consolidate performance troubleshooting into a single platform, without the manual configuration and hazards of missing elastic or burst workload changes.

Foglight Hybrid Cloud Manager for AWS simplifies the cloud performance monitoring process, allowing users to see VMware, Hyper-V, and AWS inside of a single platform. By the means of unified workflows, pre-configured rules with notifications, and intelligent analytics, Foglight Hybrid Cloud Manager for AWS unscrambles complex troubleshooting and delivers the information that helps user cut down costs.

This section introduces you to the Foglight Hybrid Cloud Manager for AWS environment, and provides you with essential information.

For more information, see the following topics:

- Installation requirements
- AWS Agent Configuration
- AWS monitoring setup
- Dashboard location and UI elements

Installation requirements

Foglight Hybrid Cloud Manager for AWS comes installed on Foglight Evolve and can be installed on a Foglight Management Server.

Foglight Hybrid Cloud Manager for AWS requires the following cartridges for data collection:

1. *vUsage-Feedback-6_0_0.car*
2. *DRP-6.0.0.car*
3. *Cloud-Manager-6.0.0.car*
4. *OptimizerAutomation-6_0_0.car*
5. *CommonAnalytics-6_0_0.car*
6. *Optimizer-6.0.0.car*

While Foglight Evolve comes with these cartridges pre-installed and enabled, a stand-alone Foglight release requires that these components be installed on the Foglight Management Server. The sequence of cartridge installation is important because of their dependencies. For more information about installing Foglight Hybrid Cloud Manager for AWS, and for details about system requirements and version compatibility, see the *Foglight Hybrid Cloud Manager Release Notes*.

AWS Agent Configuration

Minimum application privileges

Each AWS Agent monitors the assets inside the selected region. To monitor an AWS environment, AWS Identity and Access (IAM) users need to use an Access Keys to secure REST or HTTP query protocol requests. Create an IAM user with the following privileges to use the Foglight Hybrid Cloud Manager for AWS:

- *AmazonSSMFullAccess*
- *AmazonEC2ReadOnlyAccess*
- *CloudWatchFullAccess*
- *IAMReadOnlyAccess*
- *AWSHealthFullAccess*

To collect EC2 Memory metrics and Linux Volume metrics, make sure to assign the following privilege when creating the EC2 instance that will be launched and monitored:

- *AmazonEC2RoleforSSM*

To use **Optimizer Reclaim** action, it is recommended to create a custom policy to assign the following privileges to the user:

- Write access level including the following actions for EC2 service is required:
  - *ModifyInstanceAttribute*
  - *StartInstances*
  - *StopInstances*
- Write access level including the following actions for EC2 Auto Scaling service is required:
  - *ResumeProcesses*
  - *SuspendProcesses*

API used to collect Cost metrics

Foglight Hybrid Cloud Manager for AWS uses the AWS Cost and Usage Report to tracks your AWS usage and provides the estimated charges associated with your AWS account. AWS delivers the AWS Cost & Usage Report (in CSV format) for the Amazon Simple Storage Service (S3) bucket you specified, and updates the reports at least once a day. AWS Agent retrieves the reports programmatically using the Amazon S3 APIs.

If you use the consolidated billing feature in AWS Organizations, this report is available only to the master account and includes activity for all the member accounts that are associated with the master account.

Refer to the AWS Cost and Usage Report for more details.

To get Account ID (12-digit number)

1. Log in to the AWS Management Console: https://console.aws.amazon.com.
2. Locate your Account ID
   a. Click **Support** on the navigation bar on the upper-right.
   b. Choose **Support Center**. Your currently signed-in account number (ID) appears in the **Support Center** title bar.

To create an AWS Cost and Usage Report

1 Sign in to the AWS Management Console and open the Billing and Cost Management console at https://console.aws.amazon.com/billing/.

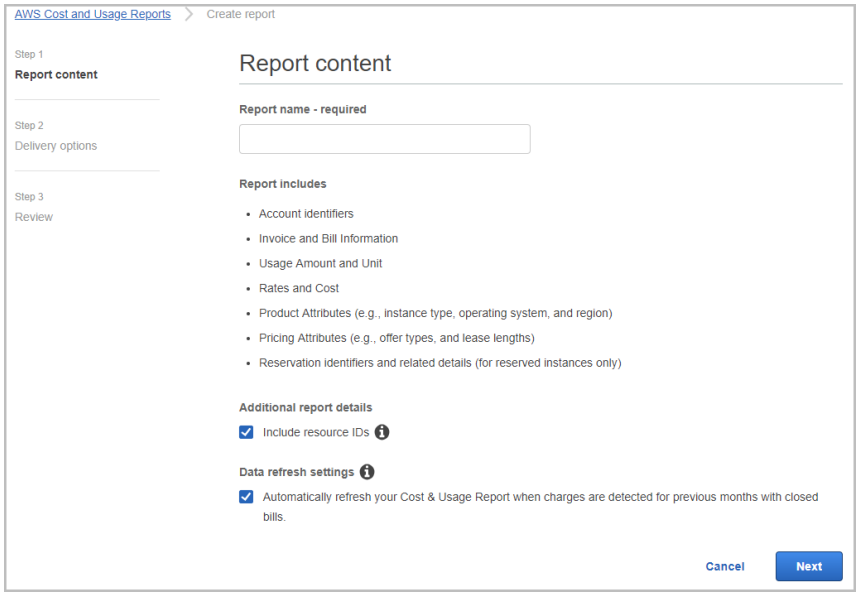
2 On the navigation pane, choose **Reports**.

3 Choose **Create report**.

4 Type the following information, as needed, and then click **Next**.

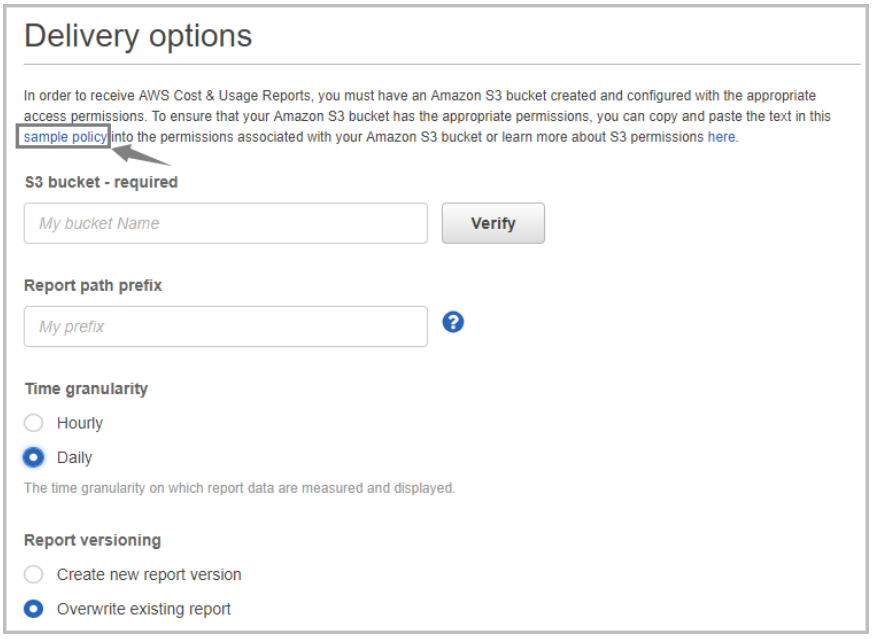
   a ***Report name***: enter the name of report.

   b *Additional report details*: select Include resource IDs.

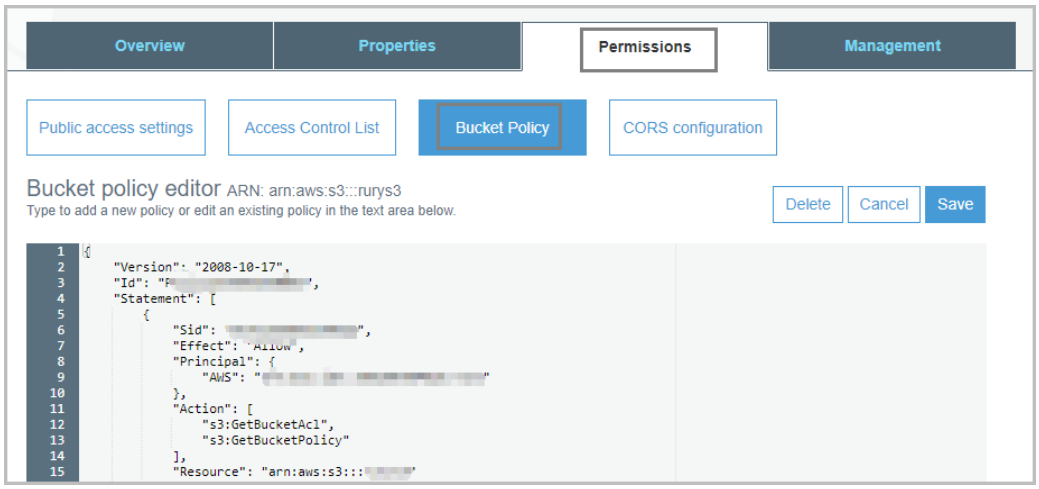


5 ***S3 bucket***: Enter the name of the **Amazon S3 bucket** where you want the reports to be delivered and then select **Verify**. The bucket must have appropriate permissions.

   a Click **Sample Policy** link and copy and paste the text in this sample policy into the permissions associated with your Amazon S3 bucket.



b Open a new Page to access your S3 bucket, click **Permissions** and then **Bucket policy**. Paste the text in this sample policy into the permissions associated with your Amazon S3 bucket.



c Below is an example for the S3 bucket policy. Update the following descriptions in bold according to your AWS Account and S3 bucket.

- AWS monitoring user ARN (in line 32): `"arn:aws:iam::88888888:user/exampleAWSUserTest":`

  Format: "arn:aws:iam::your AWS Account ID:user/your monitoring AWS username"

  To get the AWS user ARN from AWS Console, select IAM, and then click the AWS user which is configured under the Foglight AWS Agent.

- S3 bucket ARN (in line 15, 26, and 35): `"arn:aws:s3:::exampleBucketNameTest":`

  Format: arn:aws:s3:::your bucket name

  Change the exampleBucketNameTest to your S3 bucket name.

```
{
    "Version": "2008-10-17",
    "Id": "PolicyForFoglightAWSCostReport",
    "Statement": [
        {
            "Sid": "StmtForAWSBillingReportGet",
            "Effect": "Allow",
            "Principal": {
                "Service": "billingreports.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::exampleBucketNameTest"
        },
        {
            "Sid": "StmtForAWSBillingReportPut",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "billingreports.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::exampleBucketNameTest/*"
        },
        {
            "Sid": "StmtForAWSUserGet",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::88888888:user/exampleAWSUserTest"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::exampleBucketNameTest/*"
        }
    ]
}
```

6 ***Report path prefix*** - *Optional:* Enter the report path prefix that you want to name of your report.

7 Time granularity: Choose **Daily**.

8 *Report versioning*: Choose *"*Overwrite existing report*"*.

9 *Enable report data integration for*: Leave blank.

10 *Compression type*: Choose GZIP or ZIP

11 Click ***Next****, after you have reviewed the settings for your report, choose Review and Complete.*

AWS monitoring setup

A complete setup includes the following two steps:

1 Get the authentication information through AWS Management Console. For more information, see Getting authentication information through console on page 11.

2 Create an AWS Agent on the Foglight Management Server. For more information, see Creating an AWS Agent on page 12.

3 (Optional) Configure the interval of data collection. For more information, see Configuring data collection interval on page 13.

Getting authentication information through console

To create and retrieve a user's Access Keys through the AWS IAM console:

1 Log in to the AWS IAM console at: https://console.aws.amazon.com/iam/.

2 Click **IAM** under the *Security, Identity & Compliance* column.

3 On the left navigation panel, click **Users**.

The *Resource Groups* view opens on the right.

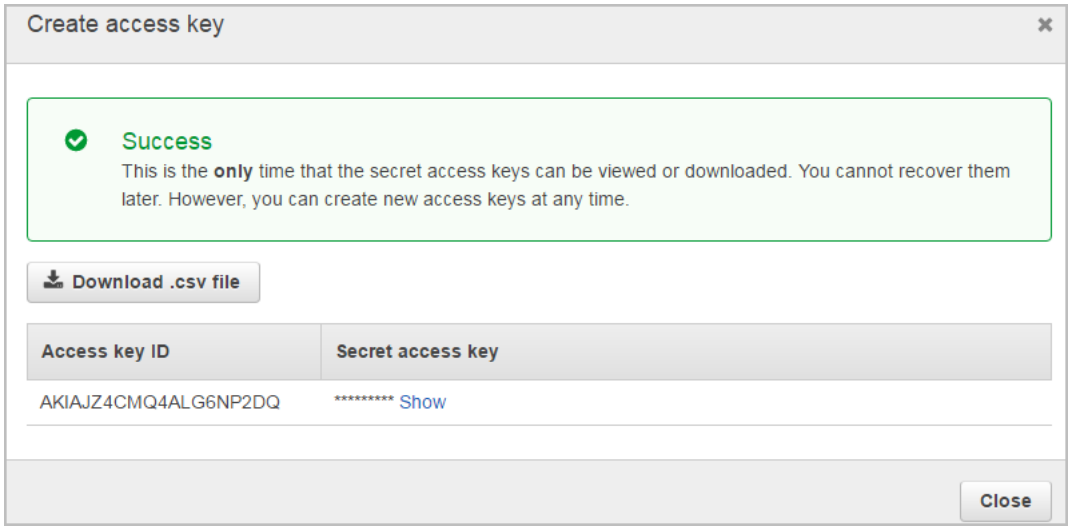
4 In the *Resource Groups* view, click the user which Access Key is to be retrieved.

The *User Summary* view opens.

5 In the *User Summary* view, click **Security credentials**, then the *Sign-in credentials* view opens.

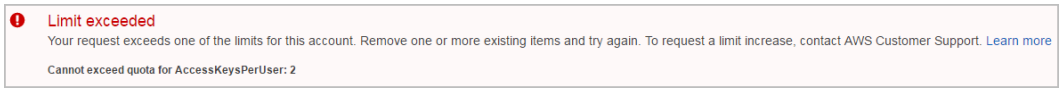
6 In the *Access keys* area, click **Create access key**.

The **Create access key** dialog box appears and shows the access key and Secret access key.



7 Click **Download .csv file** to keep the access key and secret access key somewhere safe.

8 (Optional) If you see the *Limit exceed* message, click the ✖ button next to the **Status** column to delete an access key that is not being used. Then repeat Step 6 to create and retrieve a new access key.



Configuring firewall settings

If your AWS Performance Agent is installed behind the firewall, ensure the following URL addresses and ports are open:

- URL address:
  - *.amazon.com
- TCP/UDP port:
  - 80 and 443

Creating an AWS Agent

To create an AWS agent:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

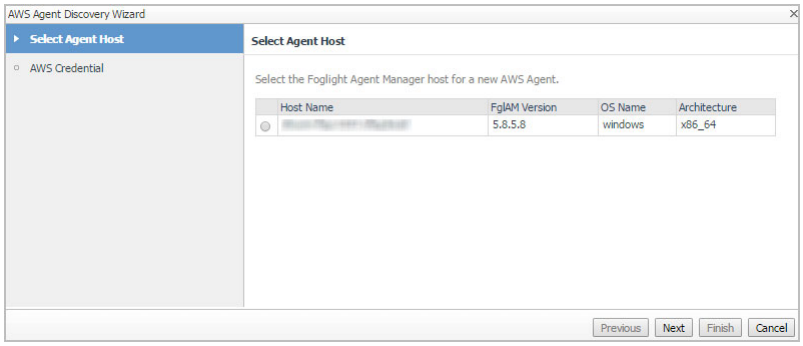
To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 In the **Cloud Manager** dashboard, click **Administration**, and then click **Add** or **Create AWS Agent**.

The **Agent Setup Wizard** dialog box opens.



5 In the *Select Agent Host* view, select the agent manager on which the new agent is to be deployed, and then click **Next**.

6 In the *AWS Credential* view, specify the following values, as needed, then click **Finish**.

- *Account Alias*: The display name of this account.
- *Access Key ID*: The access key retrieved in Getting authentication information through console.
- *Secret Access Key*: The secret access key retrieved in Getting authentication information through console.
- *Collect Memory Metric*: Select this option to enable the collection of instance memory metrics. The default value is disabled. Foglight supports to collect memory metrics for both Windows and Linux OS. To enable Linux OS Memory Metrics collection, upload the private key and assign the credential to the required instance. For how to upload private key and assign the credential to required instance, refer to To create user name and password for an instance: on page 46. No additional tasks are required when enabling Windows OS memory metrics collection.
- *Collect Linux Volume Utilization*: Select this option to enable the collection of Linux volume utilization. The default value is disabled. Foglight only supports to collect volume utilization for Linux OS. To enable Linux OS Memory Metrics collection, upload the private key and assign the credential to the required instance. For how to upload private key and assign the credential to required instance, refer to To assign credentials for AWS instances: on page 47.
- *Specify an agent name (Optional)*: Specify the name of agent.
- *Configure regions to be monitored (Optional)*: Select AWS regions for monitoring. All regions will be monitored if this field is not configured.
- *Configure Account Cost to Monitor*: Configure the Cost Metrics collection. Collections will start only after the AWS Cost and Usage Report are created on the AWS Console. See To create an AWS Cost and Usage Report. For more details, see Configure Account Cost to Monitor: on page 50.
- *Configure Proxy (Optional)*: Configure the proxy setting when the Agent Host requires a proxy connection to the Internet. For more details, see Configure Proxy (Optional): on page 51.

The new AWS Agent is created, and its data is to be displayed on the **Monitoring** tab after a few minutes.

Configuring data collection interval

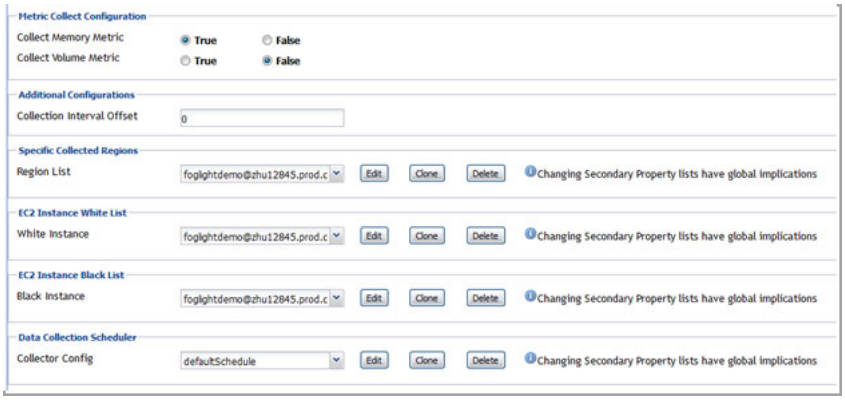
Foglight Hybrid Cloud Manager enables you to configure the interval for data collection using the *Agent Status* dashboard.

To configure the data collection interval:

1 On the navigation panel, under **Dashboards**, select **Administration > Agents > Agent Status**.

2 On the *Agent Status* dashboard, select the AWS agent that you want to monitor, and then click **Edit Properties**.

The *Edit Properties* view opens.



3 Select *True* for *Collect Memory Metric* and *Collect Volume Metric*, and then specify a value for *Collection Interval Offset*.

Quest highly recommends setting the *Collector Config (also knowns as Collection interval)* to a value greater than 10 minutes. If the Collection interval is less than 10 minutes, AWS agent cannot collect metrics from AWS Cloud Watch as AWS Cloud Watch has a 10-minute delay. If you insist on setting this interval less than 10 minutes, ensure the following:

- *Collection Interval Offset* must be set to a non-negative integer.
- The configuration should follow comply with the formula: (n+1) x I >= 10 minutes.
  - n represents the value of *Collection Interval Offset*.
  - I represents the value of *Collector Config* (in minutes).

Dashboard location and UI elements

After installing Foglight Hybrid Cloud Manager for AWS, the **Cloud Manager** entry appears under *Homes*.

To access the Cloud Manager dashboard:

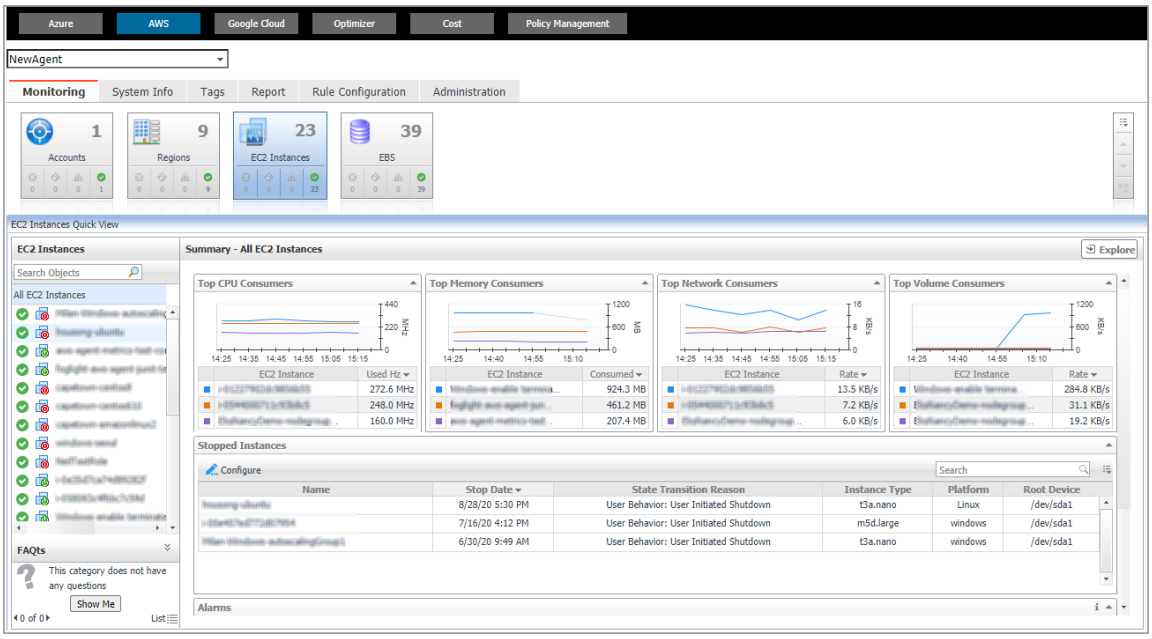
1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**, and then click **AWS**.

The **Cloud Manager** dashboard opens.



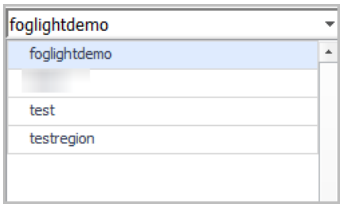
The **Cloud Manager** dashboard consists of the following UI elements:

- Group selector
- Actions bar
- Menu bar
- Quick view

Group selector

The Group selector is located at the top of the dashboard and allows you to select the AWS environment that you want to monitor.

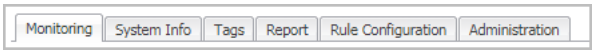
Figure 1. Group Selector



Actions bar

The actions bar at the top of the Cloud Manager dashboard contains the Monitoring Tab, the System Info Tab, the Tags Tab, the Report Tab, the Rule Configuration Tab, and the Administration Tab.

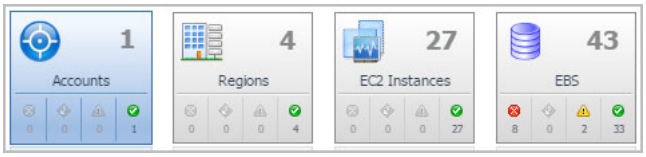
Figure 2. Actions bar



Menu bar

The Menu bar contains the following tiles: *Regions monitoring*, *Account monitoring*, *EC2 Instances Monitoring*, and *EBS monitoring*.

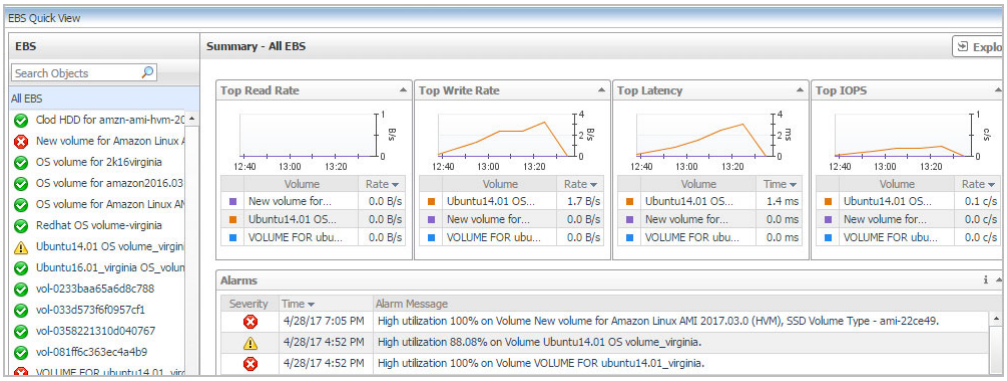
Figure 3. Menu bar



Quick view

The quick view is located on the lower part of the **Cloud Manager** dashboard, which is updated based on the tab selected on the Menu bar or the Actions bar.

Figure 4. Quick view

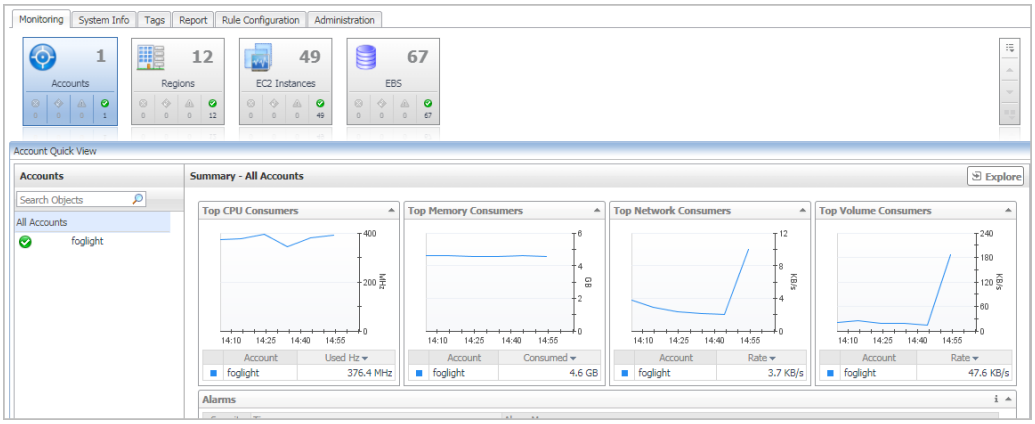


2

Monitoring Tab

When navigating to the **Cloud Manager** dashboard for the first time, the **Monitoring** tab appears. The **Monitoring** tab allows you to select a monitoring object or a group of objects, such as regions, accounts, EC2 instances, or EBS, and review the data associated with your selection.

Figure 5. Monitoring dashboard



To access the Monitoring dashboard:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**, and then click **AWS**.

   The **Cloud Manager** dashboard opens
4. On the actions bar, click **Monitoring**.
5. Select the **Regions**, **Accounts**, **EC2 Instances,** or **EBS** tile from the top left.

For more information, see the following topics:

- Regions monitoring
- Account monitoring
- EC2 Instances Monitoring
- EBS monitoring

Regions monitoring

The Regions view shows the data collected about a specific region or all AWS regions. For more information, see the following topics:

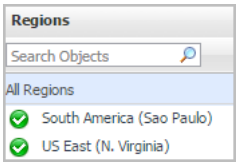
- Regions view

- Summary - All Regions view
- Explore - All Regions view
- Region Summary view
- Region Explore view

Regions view

The **Regions** tree view lists the regions existing in your AWS environment and shows their state. This view appears on the left when you select the **Regions** tile in the Actions bar.

Figure 6. Regions view



Selecting the **All Regions** node displays the Summary - All Regions view on the right. Similarly, selecting a region node shows region-specific metrics in the Region Summary view on the right.

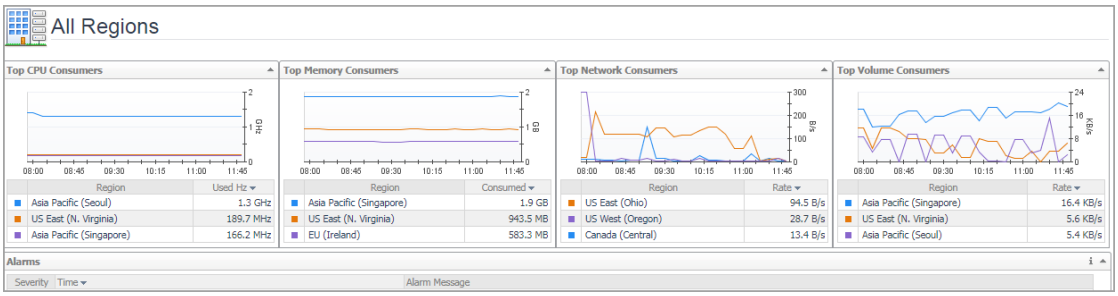
Table 1. Description of the View

Data displayed	• **Alarm severity**. The state of the most recent alarm raised against the associated virtual machine. • **All Regions**. A parent node for the regions that appear in this view. • **Region**. The region name.
Where to go next	Drill down on: • **All Regions**. Shows the Summary - All Regions view on the right. • **Region**. Shows the Region Summary view on the right.

Explore - All Regions view

The Explore - All Regions view appears when you click **Explore** in the Summary - All Regions view.

Figure 7. Explore - All Regions view



This view consists of the following embedded views:

- Alarms
- Top 3 Consumers

Table 2. Alarms

Description	Lists the alarms generated against the selected virtual machine.
Data displayed	• **Alarm Message**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Time.** Indicates when the alarm occurred.
Where to go next	Drill down on: • **Alarm Message, Severity**, or **Time**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

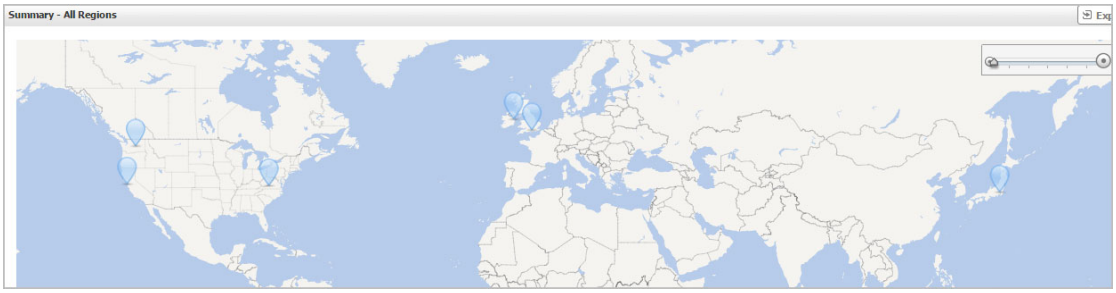
Table 3. Top 3 Consumers

Description	Shows the top three consumers in all regions.
Data displayed	• **CPU Consumers**. Indicates top 3 CPU Utilization usage regions. • **Memory Consumers**. Indicates top 3 memory usage regions. • **Network Consumers.** Indicates top 3 network usage regions. • **Volume Consumers.** Indicates top 3 volume usage regions.
Where to go next	Drill down on: • Click the Region to drill down to region explore view.

Summary - All Regions view

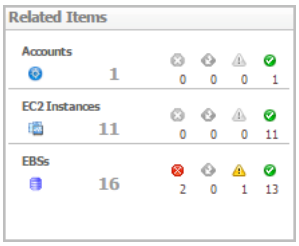
The **Summary - All Regions** view appears on the right when you select **All Regions** in the Regions view.

Figure 8. Summary - All Virtual Machines view



Hover over any bubble in this graph to display a dwell, showing *Accounts, EC2 Instances, and EBSs*.

Figure 9. Region dwell

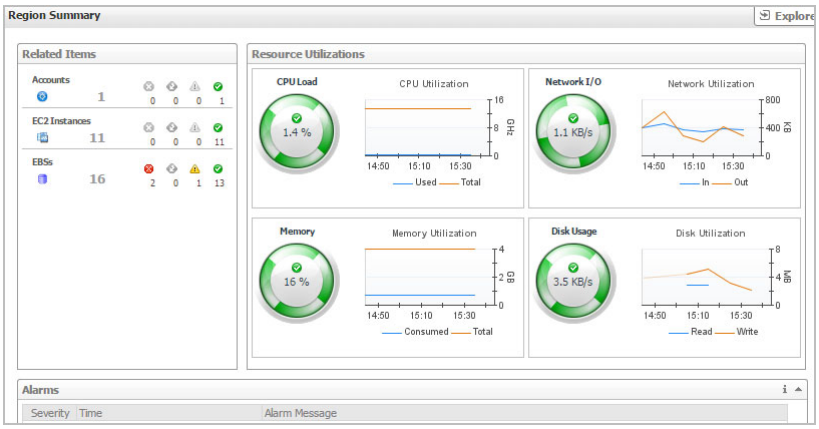


Click any bubble in this graph to open the Region Summary view, showing *Related Items, Resource Utilization,* and *Alarms.*

Region Summary view

The **Region Summary** view appears on the right when you select a region in the Regions view.

Figure 10. Region Summary view



This view consists of the following embedded views:

- Alarms
- Related Items
- Resource Utilization

Table 4. Alarms

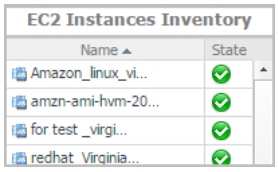
Description	Lists the alarms generated against the selected virtual machine.
Data displayed	• **Alarm Message**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Time.** Indicates when the alarm occurred.
Where to go next	Drill down on: • **Alarm Message, Severity**, or **Time**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

Table 5. Related Items

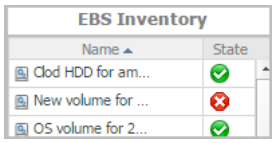
Description	Shows the numbers and states of the selected regions.
Data displayed	• **EC2 Instances**. The number of the ECS2 instances that are associated with the selected region, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal). • **EBSs**. The number of the EBSs that are associated with the selected region, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal). • **Accounts.** The number of the accounts that are that are associated with the selected region, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal).
Where to go next	Drill down on:

Table 5. Related Items

- **EC2 Instances**. Displays the **EC2 Instances Inventory** dwell, showing the name and state of the associated Resource Groups.



- **EBSs**. Displays the **EBS Inventory** dwell, showing the name and state of the associated virtual machine.



- **Accounts**. Displays the **Other Items Inventory** dwell, showing the name and state of the associated accounts.

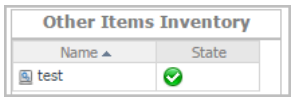


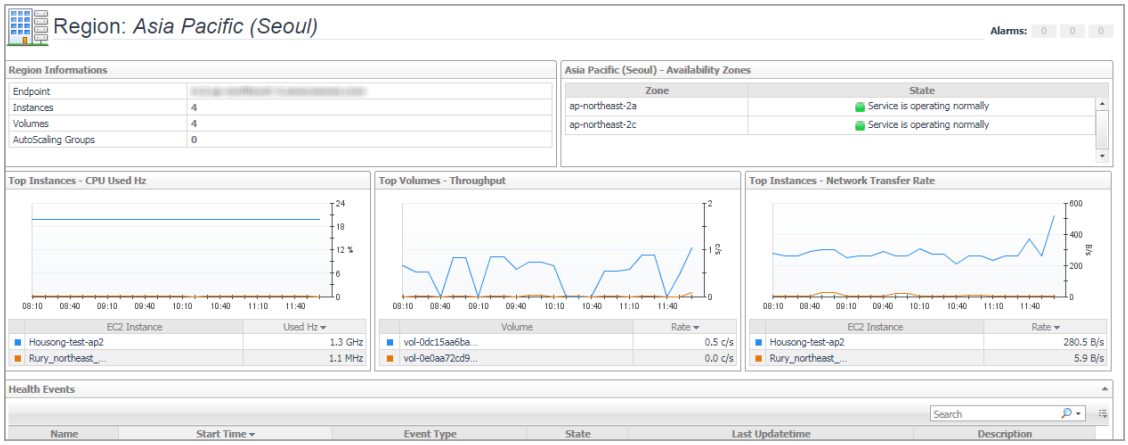
Table 6. Resource Utilization

Description	Shows a table, showing the information about the resource utilization associated with the selected region.
Data displayed	• **Disk Usage**. Indicates total Disk Usage throughput across all EC2 Instances monitored by the Region. • **Network I/O**. Indicates total network throughput across all EC2 Instances monitored by the Region. • **CPU Load**. Shows the average CPU Load on all EC2 Instances for the Region based on the total capacity. • **Memory**. Shows the Memory Utilization summary for the specified Region based on the total capacity.
Where to go next	Drill down on: • **CPU Load**. Displays the **CPU Load** dialog box, including *CPU Utilization* and *Baseline*. • **Memory**. Displays the **Memory Usage** dialog box, including *Memory Utilization* and *Baseline*. • **Network I/O**. Displays the **Network I/O** view, showing the metrics of *network Usage (in bps)* and *Baseline*. • **Disk Usage**. Display the **Disk Usage** view, showing the metrics of *disk Usage* and *Baseline*.

Region Explore view

The *Region Explore* view opens when you click **Explore** in the Region Summary view.

Figure 11. Region Explore view



This view consists of the following embedded views:

- Region Information
- Region Availability Zones
- Top Consumers
- Health Events

Table 7. Region Information

Description	Shows region basic information, include endpoints, instances, volumes, and auto scaling groups.

Table 8. Region Availability Zones

Description	Shows the state of the availability zones.

Table 9. Top Consumers

Description	Show the top 3 consumers at this region.
Data displayed	• **Top Instances - CPU Used Hz**. Indicates top 3 CPU Usage at this region. • **Top Volumes - Throughput**. Indicates top 3 volume throughput at this region. • **Top Instances - Network Transfer Rate**. Indicates top 3 network transfer rate at this region.
Where to go next	Drill down on: • Click the instance name to drill down to instance explore view. • Click the volume name to drill down to volume explore view.

Table 10. Health Events

Description	Shows health events belong to this region, include the event name, start time, event type, and so on.

Account monitoring

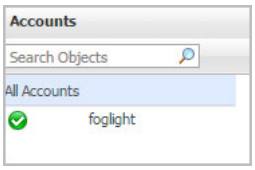
The Accounts view shows the data collected about a specific account created by IAM users. For more information, see the following topics:

- Accounts view
- Summary - All Accounts view
- Account Summary view

Accounts view

The **Accounts** tree view lists the account existing in your AWS environment and shows their state. This view appears on the left when you select the **Accounts** tile in the Actions bar.

Figure 12. Accounts view



Selecting the **All Accounts** node displays overall resource utilization for all accounts in your AWS environment and the elements that consume the highest amount of system resources in the Summary - All Accounts view on the right. Similarly, selecting an account node shows account-specific metrics in the Account Summary view on the right.

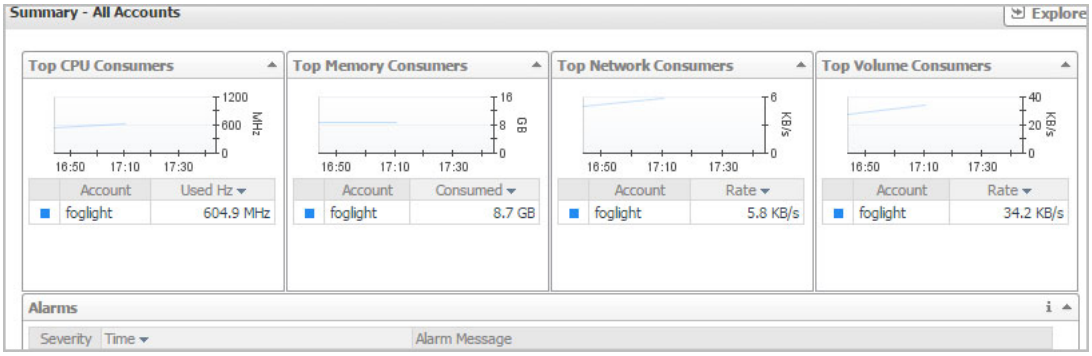
Table 11. Description of the View

Data displayed	• **Alarm severity**. The state of the most recent alarm raised against the associated account. • **All Accounts**. A parent node for the account object instances that appear in this view. • **Account**. The account name.
Where to go next	Drill down on: • **All Accounts**. Shows the Summary - All Accounts view on the right. • **Account**. Shows the Account Summary view on the right.

Summary - All Accounts view

The **Summary - All Accounts** view displays overall resource utilization information for a group of accounts and shows the elements that consume the highest amount of system resources. This view appears on the right when you select **All Accounts** in the Accounts view.

Figure 13. Summary - All Accounts view



This view consists of the following embedded views:

- Alarms
- Top CPU Consumers
- Top Network Consumers
- Top Memory Consumers
- Top Volume Consumers

Table 12. Alarms

Description	Lists the alarms generated against the monitored account.
Data displayed	• **Alarm Message**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Time**: Indicates when the alarm occurred.
Where to go next	Drill down on: • **Alarm Message, Severity**, or **Time**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

Table 13. Top CPU Consumers

Description	Shows the top three accounts with the highest average CPU utilization.
Data displayed	• **Utilization**. The amount of CPU processing speed each of the top three CPU consumers spend on executing system code and user programs, during the selected time range. • **Account**. The name of the account.
Where to go next	Drill down on: • **Account**. Displays the fundamental account information, including *Resource Information*, *CPU*, *Memory*, *Network*, and *Storage*.

Table 14. Top Network Consumers

Description	Shows the top three accounts that are consuming most network bandwidth.
Data displayed	• **Rate**. The rate at which the top three network consumers transfer data to or from the network during the selected time range. • **Account**. The name of the account that is one of the top three network consumers.
Where to go next	Drill down on: • **Account**. Displays the fundamental account information, including *Resource Information*, *CPU*, *Memory*, *Network*, and *Storage*.

Table 15. Top Memory Consumers

Description	Shows the top three accounts with the highest average memory utilization.
Data displayed	• **Account**. The name of the virtual machine that is one of the top three memory consumers. • **Rate**. The amount of memory the top three memory consumers use during the selected time range.
Where to go next	Drill down on: • **Account** or **Rate**. Displays the fundamental account information, including *Resource Information*, *CPU*, *Memory*, *Network*, and *Storage*.

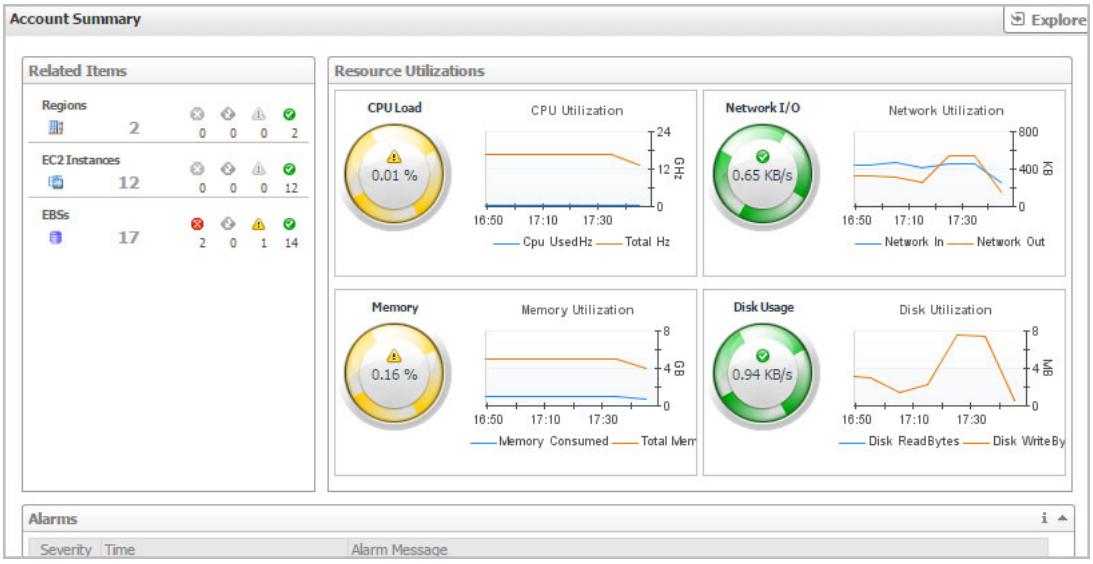
Table 16. Top Volume Consumers

Description	Shows the top three accounts with the highest available disk space.
Data displayed	• **Account**. The name of the account that is one of the top three disk consumers. • **Rate.** The rate at which the top three disk consumers read or write data to the storage during the selected time range.
Where to go next	Drill down on: • **Account** or **Rate**.Displays the fundamental VM information, including *Resource Information*, *CPU*, *Memory*, *Network*, and *Storage*.

Account Summary view

The **Account Summary** view shows the overall resource utilization and the amounts of system resource consumption for an account. This view appears on the right when you select a virtual machine in the Accounts view.

Figure 14. Account Summary view



This view consists of the following embedded views:

- Alarms
- Resource Utilization
- Related Items

Table 17. Alarms

Description	Lists the alarms generated against the selected account.
Data displayed	• **Alarm Message**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Time.** Indicates when the alarm occurred.
Where to go next	Drill down on: • **Alarm Message, Severity**, or **Time**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

Table 18. Resource Utilization

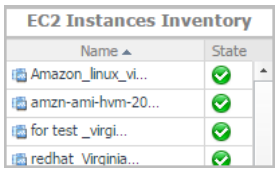
Description	Shows the numbers and states of the selected account running on the monitored AWS environment.
Data displayed	• **Disk Usage**. Indicates total Disk Usage throughput across all EC2 Instances monitored by the Region. • **Network I/O**. Indicates total network throughput across all EC2 Instances monitored by the Region. • **CPU Load**. Shows the average CPU Load on all EC2 Instances for the Region based on the total capacity. • **Memory**. Shows the Memory Utilization summary for the specified Region based on the total capacity.
Where to go next	Drill down on: • **CPU Load**. Displays the **CPU Load** dialog box, including *CPU Utilization* and *Baseline*. • **Memory**. Displays the **Memory Usage** dialog box, including *Memory Utilization* and *Baseline*. • **Network I/O**. Displays the **Network I/O** view, showing the metrics of *network Usage (in bps)* and *Baseline*. • **Disk Usage**. Display the **Disk Usage** view, showing the metrics of *disk Usage* and *Baseline*.

Table 19. Related Items

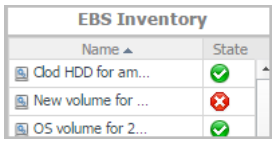
Description	Shows the resource consumption for the selected account, broken down into three simple views.
Data displayed	• **EC2 Instances**. The number of the ECS2 instances that are associated with the selected account, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal). • **EBSs**. The number of the EBSs that are associated with the selected account, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal). • **Regions.** The number of the regions that are that are associated with the selected account, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal).
Where to go next	Drill down on:

Table 19. Related Items

- **EC2 Instances**. Displays the **EC2 Instances Inventory** dwell, showing the name and state of the associated Resource Groups.



- **EBSs**. Displays the **EBS Inventory** dwell, showing the name and state of the associated virtual machine.



- **Regions**. Displays the **Regions Inventory** dwell, showing the name and state of the associated accounts.

EC2 Instances Monitoring

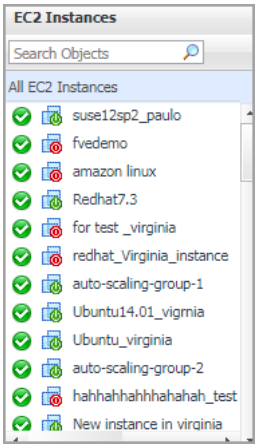
The EC2 Instances view shows the data collected about a specific EC2 instance or all EC2 instances. For more information, see the following topics:

- EC2 Instances view
- Summary - All Accounts view
- Account Summary view

EC2 Instances view

The **EC2 Instances** tree view lists the EC2 instances existing in your AWS environment and shows their state. This view appears on the left when you select the **EC2 Instances** tile in the Actions bar.

Figure 15. EC2 Instances view



Selecting the **All EC2 Instances** node displays all EC2 instances in the Summary - All EC2 Instances view on the right. Similarly, selecting an EC2 instance shows EC2 instance-specific metrics in the EC2 Instance Summary view on the right.

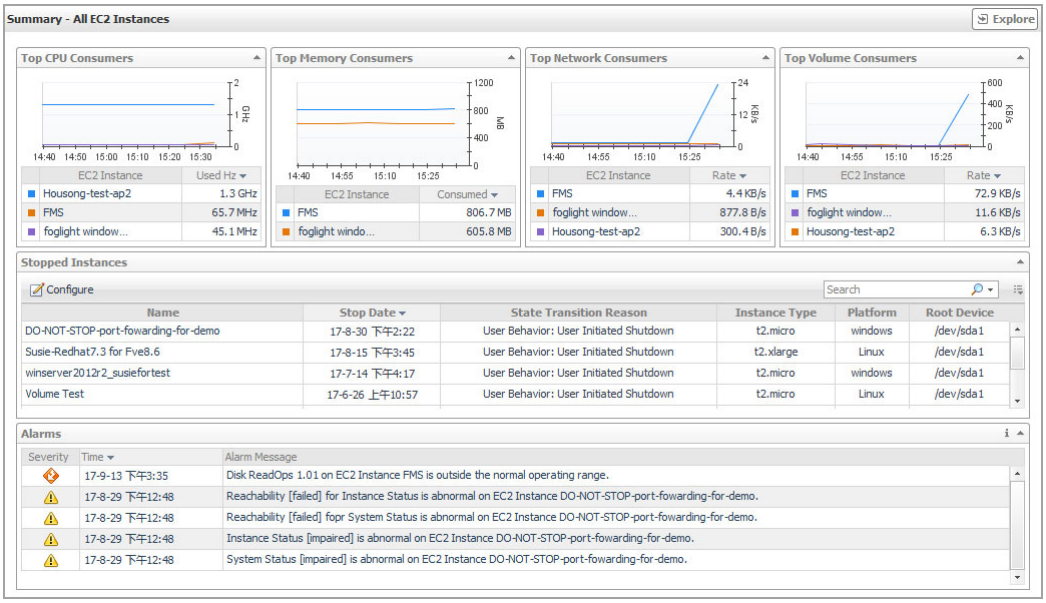
Table 20. Description of the View

Data displayed	• **Alarm severity**. The state of the most recent alarm raised against the associated EC2 instance. • **All EC2 Instances**. A parent node for the EC2 instances that appear in this view. • **EC2 Instance**. The EC2 instance name. • **EC2 Instance Power state**. The EC2 instance power state.
Where to go next	Drill down on: • **All EC2 Instances**. Shows the Summary - All EC2 Instances view on the right. • **EC2 Instance**. Shows the EC2 Instance Summary view on the right.

Summary - All EC2 Instances view

The **Summary - All EC2 Instances** view displays overall EC2 instance information. This view appears on the right when you select **All EC2 Instances** in the EC2 Instances view.

Figure 16. Summary - All EC2 Instances view



This view consists of the following embedded views:

- Alarms
- Top CPU Consumers
- Top Network Consumers
- Top Memory Consumers
- Top Volume Consumers
- Stopped Instances

Table 21. Alarms

Description	Lists the alarms generated against the monitored virtual machine.
Data displayed	• **Description**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Title**: Indicates the alarm title. • **Ack'ed**. Indicates whether the alarm was acknowledged.
Where to go next	Drill down on: • **Description, Severity**, **Title**, or **Ack'ed**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

Table 22. Top CPU Consumers

Description	Shows the top three EC2 instances with the highest average CPU utilization.
Data displayed	• **Utilization**. The amount of CPU processing speed each of the top three CPU consumers spend on executing system code and user programs, during the selected time range. • **EC2 Instance**. The name of the EC2 instance.

Table 23. Top Network Consumers

Description	Shows the top three EC2 instances that are consuming most network bandwidth.
Data displayed	• **Rate**. The rate at which the top three network consumers transfer data to or from the network during the selected time range. • **EC2 Instance**. The name of the EC2 instance that is one of the top three network consumers.

Table 24. Top Memory Consumers

Description	Shows the top three EC2 instances with the highest average memory utilization.
Data displayed	• **EC2 Instance**. The name of the EC2 instance that is one of the top three memory consumers. • **Rate**. The amount of memory the top three memory consumers use during the selected time range.

Table 25. Top Volume Consumers

Description	Shows the top three EC2 instances with the highest average volume utilization.
Data displayed	• **Rate**. The rate at which the top three volume consumers transfer data to or from the network during the selected time range. • **EC2 instance**. The name of the EC2 instance that is one of the top three volume consumers.

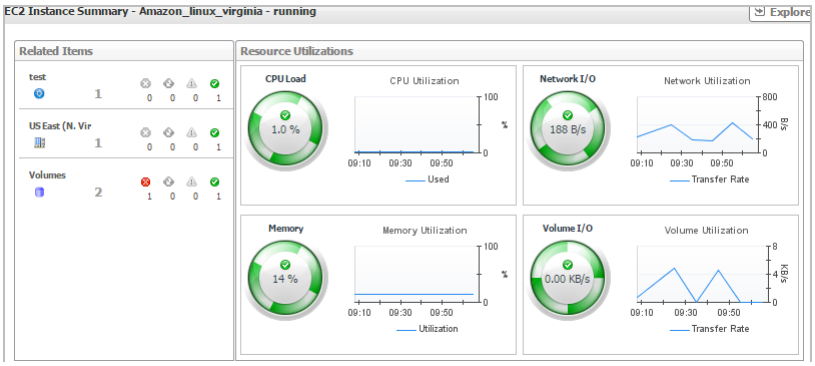
Table 26. Stopped Instances

Description	Shows stopped instances based on the configurations.
Data displayed	• **Table**. Shows the instance name, stop date, reason and so on. • **Configure**. Configures the days to judge which instances are stopped instances.

EC2 Instance Summary view

The **EC2 Instance Summary** view shows the overall information of the selected EC2 instance. This view appears on the right when you select an EC2 instance in the EC2 Instances view.

Figure 17. EC2 Instance Summary view



This view consists of the following embedded views:

- Alarms

- Related Items

Table 27. Alarms

Description	Lists the alarms generated against the selected EC2 instance.
Data displayed	• **Alarm Message**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Time.** Indicates when the alarm occurred.
Where to go next	Drill down on: • **Alarm Message, Severity**, or **Time**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

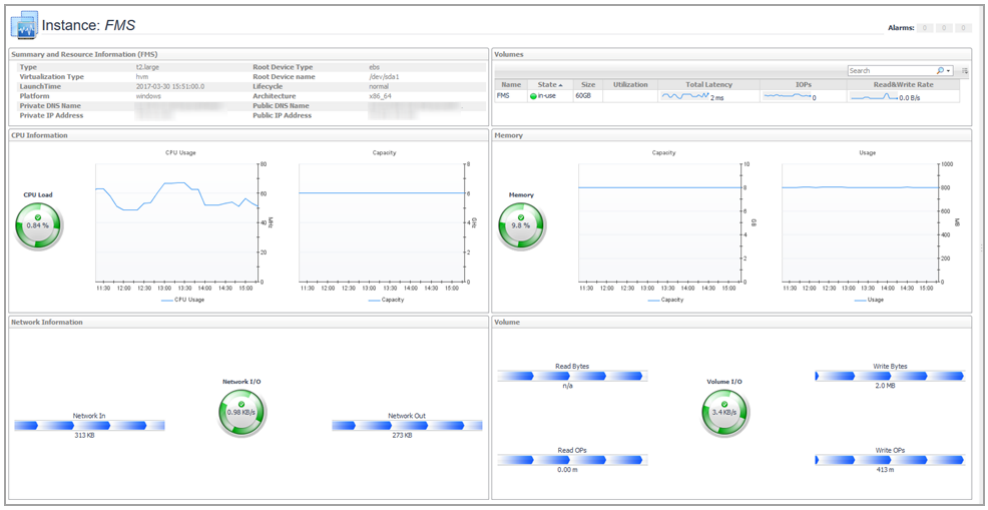
Table 28. Related Items

Description	Shows the numbers and states of the selected resource group on the monitored AWS environment.
Data displayed	• **Disk Usage**. Indicates total Disk Usage throughput across all EC2 Instances monitored by the Region. • **Network I/O**. Indicates total network throughput across all EC2 Instances monitored by the Region. • **CPU Load**. Shows the average CPU Load on all EC2 Instances for the Region based on the total capacity. • **Memory**. Shows the Memory Utilization summary for the specified Region based on the total capacity.
Where to go next	Drill down on: • **CPU Load**. Displays the **CPU Load** dialog box, including *CPU Utilization* and *Baseline*. • **Memory**. Displays the **Memory Usage** dialog box, including *Memory Utilization* and *Baseline*. • **Network I/O**. Displays the **Network I/O** view, showing the metrics of *network Usage (in bps)* and *Baseline*. **Disk Usage**. Display the **Disk Usage** view, showing the metrics of *disk Usage* and *Baseline*.

Explore - Instance view

The **Explore - Instance** view appears when you click **Explore** in the EC2 Instance Summary view.

Figure 18. Explore - Instances view



This view consists of the following embedded views:

- Summary and Resource Information
- Volumes
- CPU Information
- Memory
- Network Information

Table 29. Volumes

Description	Shows the volumes that used by this instance. Table will show the name, state, size, utilization and so on.
Where to go next	Drill down on: • **Description, Severity**, **Title**, or **Ack'ed**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

Table 30. CPU Information

Description	.Shows CPU capacity, usage, and utilization.
Data displayed	• **Utilization**. Jumps to the **Utilization** dialog box. • **Usage**. Jumps to the **Usage** dialog box. • **Capacity**. Jumps to the **Capacity** dialog box.

Table 31. Memory

Description	Shows Memory capacity, usage and utilization.
Data displayed	• **Utilization**. Jumps to the **Utilization** dialog box. • **Usage**. Jumps to the **Usage** dialog box. • **Capacity**. Jumps to the **Capacity** dialog box.

Table 32. Network Information

Description	Shows Network in, Network out, and transfer rate.
Data displayed	• **Network in**: Jumps to the **Network in** dialog box. • **Network out**. Jumps to the **Network out** dialog box. • **Transfer rate**. Jumps to the **Transfer rate** dialog box.

Table 33. Summary and Resource Information

Description	Shows the basic information about the selected EC2 instance, including EC2 instance type, name and type of the root device, DNS name, IP address and so on.

Table 34. Volume

Description	Shows Total volume read bytes, write bytes, and utilization.
Data displayed	• **Read bytes:** Jumps to the **Read bytes** dialog box. • **Write bytes.** Jumps to the **Write bytes** dialog box. • **Utilization**. Jumps to the **Utilization** dialog box.

EBS monitoring

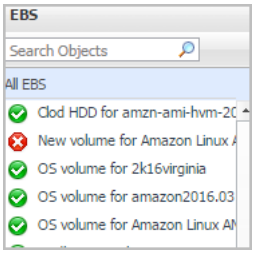
The EBS view shows the data collected about a specific EBS or all EBSs. For more information, see the following topics:

- EBS view
- Summary - All EBS view
- EBS Summary view

EBS view

The **EBS** view is a tree view. It lists the EBS instances existing in your environment, and shows their severity state.This view appears on the left when you select the **EBS** tile in the Actions bar.

Figure 19. EBS view



Selecting the **All EBS** node displays the overall resource utilization for all EBS instances in your integrated system and identifies the ones that consume the highest amount of system resources in the Summary - All EBS view on the right. Similarly, selecting a storage node shows storage-specific metrics in the EBS Summary view.

Table 35. Description of the View

Data displayed	• **Alarm severity**. The state of the most recent alarm raised against the EBS instance. • **All EBS**. A parent node for all EBS instances that appear in this view.

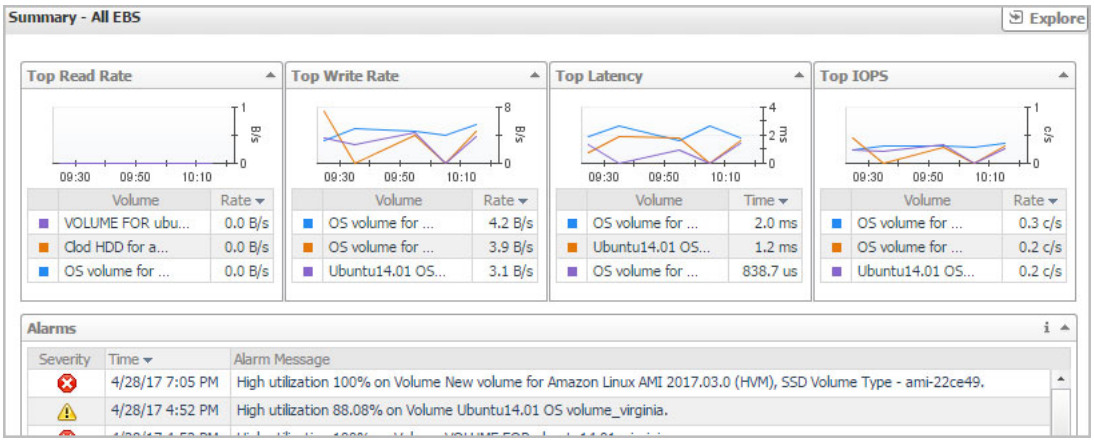
Table 35. Description of the View

	• **EBS**. The EBS instance.
Where to go next	Drill down on: • **All EBS**. Shows the Summary - All EBS view on the right. • **EBS**. Shows the EBS Summary view on the right.

Summary - All EBS view

The **Summary - All EBS** view displays overall information for all EBS instances in the selected service and identifies the elements that consume the highest amount of resources. This view appears on the right when you select **All EBS** in the EBS view.

Figure 20. Summary - All EBS view



This view consists of the following embedded views:

- Alarms
- Top Read Rate
- Top Write Rate
- Top Latency
- Top Latency

Table 36. Alarms

Description	Lists the alarms generated against the monitored EBS.
Data displayed	• **Alarm Message**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Time**: Indicates when the alarm occurred.
Where to go next	Drill down on: • **Alarm Message, Severity**, or **Time**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

Table 37. Top Read Rate

Description	Shows the top three EBS instances with the highest read rate.
Data displayed	• **Rate**. The value of read rate (in B/s). • **Volume**. The name of the EBS instance.

Table 38. Top Write Rate

Description	Shows the top three EBS instances with the highest write rate.
Data displayed	• **Rate**. The value of write rate (in B/s). • **Volume**. The name of the EBS instance.

Table 39. Top Latency

Description	Shows the top three EBS instances with the highest latency.
Data displayed	• **Time**. The value of latency (in milliseconds). • **Volume**. The name of the EBS instance.

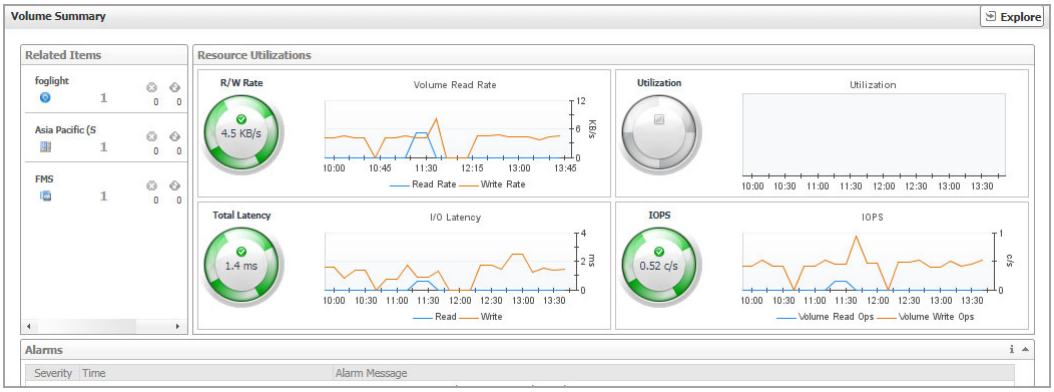
Table 40. Top IOPS

Description	Shows the top three EBS instances with the highest IOPS.
Data displayed	• **Current**. The value of IOPS (in c/s). • **Volume.** The name of the EBS instance.

EBS Summary view

The **EBS Summary** view displays complete details for an EBS instance. This view appears on the right when you select an EBS instance in the EBS view.

Figure 21. EBS Summary view



This view consists of the following embedded views:

- Alarms
- Related Items
- Resource Utilization

Table 41. Alarms

Description	Lists the alarms generated against the selected EBS instance.
Data displayed	• **Alarm Message**. An explanation about why the alarm occurred. • **Severity**. Indicates the alarm severity: Warning, Critical, or Fatal. • **Time.** Indicates when the alarm occurred.

Table 41. Alarms

Where to go next	Drill down on: • **Alarm Message, Severity**, or **Time**. Displays the **Alarm Created** dialog box, showing additional information about the alarm. For more information about alarms, see the *Foglight User Help*.

Table 42. Related Items

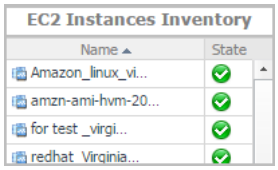
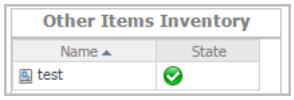
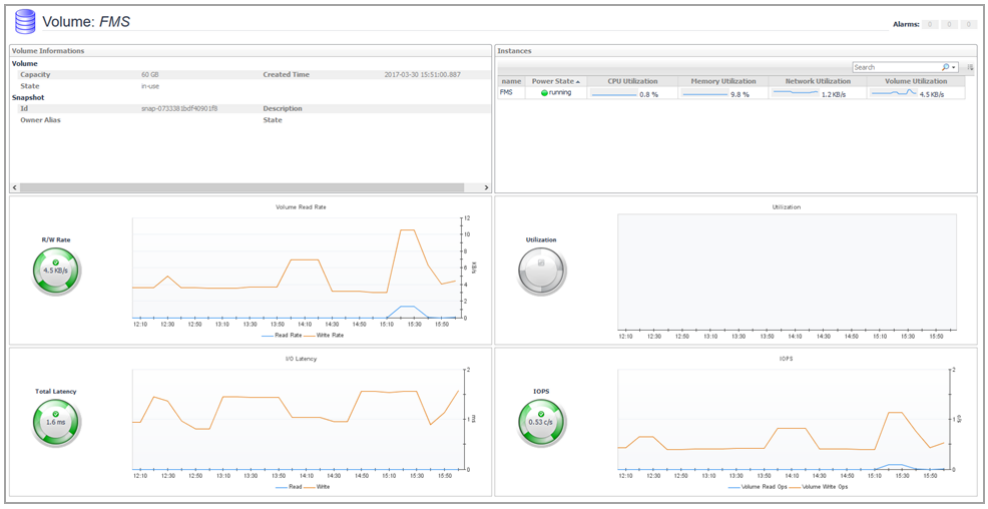
Description	Shows the numbers and states of the selected EBS instance running on the monitored AWS environment.
Data displayed	• **EC2 Instances**. The number of the ECS2 instances that are associated with the selected account, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal). • **Regions.** The number of the regions that are that are associated with the selected account, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal). • **Accounts.** The number of the accounts that are that are associated with the selected region, followed by related alarm counts, broken down by the alarm state (Normal, Warning, Critical, Fatal).
Where to go next	Drill down on: • **EC2 Instances**. Displays the **EC2 Instances Inventory** dwell, showing the name and state of the associated Resource Groups.  • **Regions**. Displays the **Regions Inventory** dwell, showing the name and state of the associated accounts.  • **Accounts**. Displays the **Other Items Inventory** dwell, showing the name and state of the associated accounts. 

Table 43. Resource Utilization

Description	Shows the resource utilization of the selected EBS instance, broken down into four simple views.
Data displayed	• **R/W Rate**. Shows the total read/write bytes per second of the selected EBS instance. • **Utilization**. Shows the disk space utilization of the selected EBS instance. • **Total Latency**. Shows the total latency the selected EBS instance. • **IOPS**. Shows the IOPS of the selected EBS instance.

Explore - Volume view

The *Explore - Volume* view appears when you click **Explore** in the EBS Summary view.



This view includes the following embedded views.

- Volume Information
- Resource Utilization
- Instance

Table 44. Resource Utilization

Description	Shows the resource utilization of the selected EBS instance, broken down into four simple views.
Data displayed	• **R/W Rate**. Shows the total read/write bytes per second of the selected EBS instance. • **Utilization**. Shows the disk space utilization of the selected EBS instance. • **Total Latency**. Shows the total latency the selected EBS instance. • **IOPS**. Shows the IOPS of the selected EBS instance.

Table 45. Volume Information

Description	Shows the volume, attachment, instance, and snapshot of the selected EBS instance.

Table 46. Instance

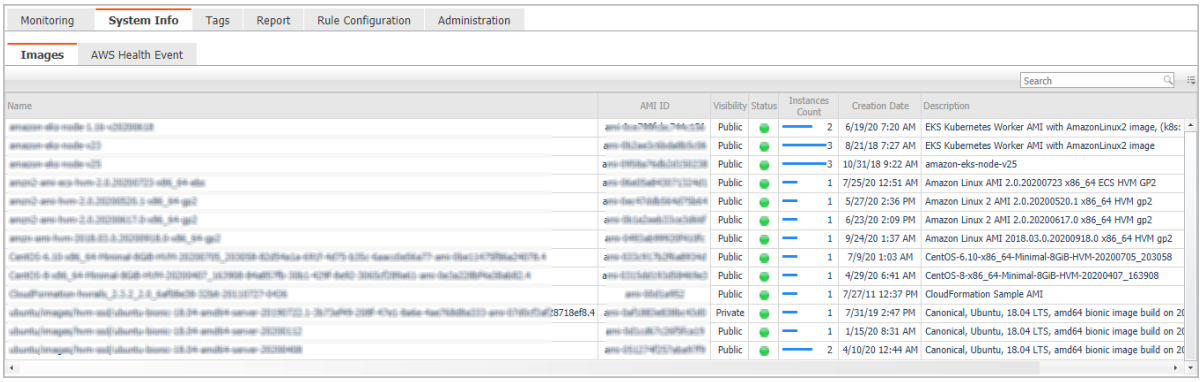
Description	Shows the instance that use this volume, will show instance name, power state, CPU utilization, and so on.

3

System Info Tab

The **System Info** tab of the **Cloud Manager** dashboard contains the Images and AWS Health Event tables to help you understand the monitored AWS environment.

Figure 22. System Info dashboard



To access the System Info dashboard:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **System Info** in the actions bar.

   The **System Info** view opens on the bottom of **Cloud Manager** dashboard.

For more information, see the following topics:

- Images table
- AWS Health Event table

Table 47. Images table

Data displayed	• **Name**. Shows the image name. • **AMI ID**. Shows the image ID. • **Visibility**. Indicates whether the image is public or private. • **Status**. Indicates whether the image is available or pending. • **Instances Count**. Shows the total number of EC2 instances that are created by this Amazon Machine Image (AMI). • **Creation Date**. Indicates when this image is created. • **Description**. Shows the description of this image.

Table 48. AWS Health Event table

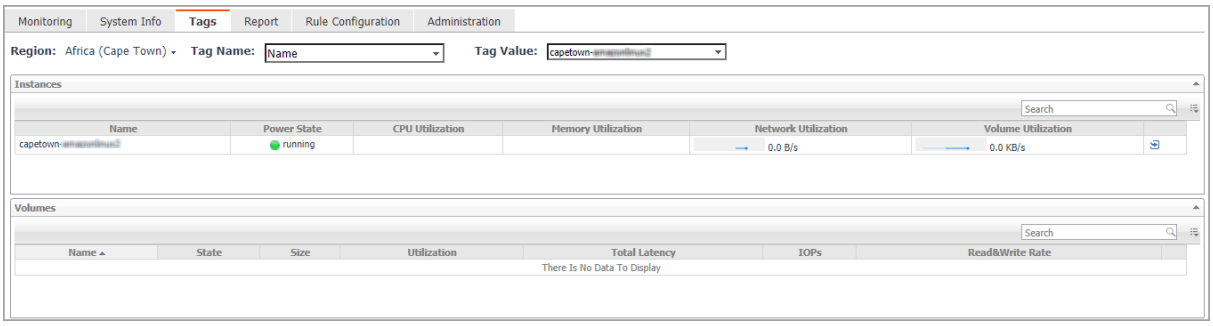
Data displayed	• **Name**. Shows the event name. • **Region**. Indicates the region in which the event occurred. • **Event Type**. Indicates the event type. • **Status**. Indicates the event status. • **Last Update**. Shows the date when the event was last updated. • **Description**. Shows the event descriptions.

4

Tags Tab

The **Tags** tab of the **Cloud Manager** dashboard helps you quickly search for instances or volumes using tag name and tag values.

Figure 23. Tags dashboard



To access the Tags dashboard:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 Click **Tags** in the actions bar.

The **Tags** view opens on the bottom of **Cloud Manager** dashboard.

The Hybrid Cloud Manager for AWS provides the following query options:

- **Region**. Lists all regions or available regions, for example, Singapore.
- **Tag Name**. Sort out all tags that belong to the selected Region.
- **Tag Value**. Sort out all tags that belong to the selected Tag Name.

The *Instances* table shows N*ame, Power State, CPU Utilization, Memory Utilization, Network Utilization*, and *Volume Utilization* of the instances that include the specified tag name or value. The *Volumes* table shows *Name, State, Size, Utilization, Total Latency, IOPS,* and *Read&Write Rate* of the instances that include the specified tag name or value.

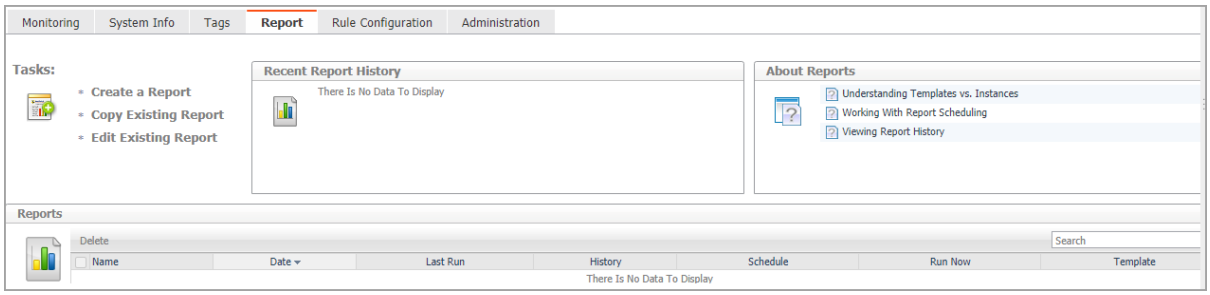
5

Report Tab

Foglight Hybrid Cloud Manager for AWS includes a report generation ability. This allows you to create reports using a set of predefined templates to report on the various aspects of your cloud environment. Foglight Hybrid Cloud Manager for AWS includes a collection of predefined report templates.

You can generate, copy, and edit reports using the Reports tab on the *Report* dashboard, or alternatively the *Reports* dashboard included with the Management Server.

Figure 24. Report dashboard



To access the Report dashboard:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **Report** in the actions bar.

For complete information about this tab, see the *Managing Capacity in Virtual Environments User Guide*. For more information about the *Reports* dashboard, see the *Foglight User Help*.

Available report templates

The following templates are available with Foglight Hybrid Cloud Manager for AWS.

Table 49. Report templates

Report Template Name	This template can be used to generate a report that…
Account Information - Summary	Summarizes your Account infrastructure, so that you could know your account's performance.
All Regions - Summary	Summarizes all regions at under your account, so that you could know all regions' performance.
AWS Optimizer - All Reports	Summarizes the AWS Optimizer resources.

Table 49. Report templates

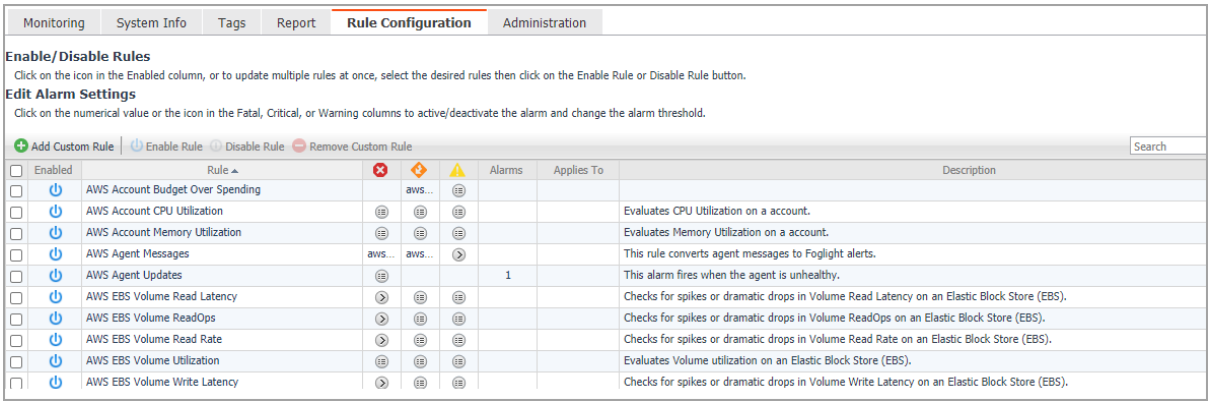
Report Template Name	This template can be used to generate a report that…
AWS Optimizer - Potential Zombie VMs Reports	Summarizes the potential zombie VM resources.
AWS Optimizer - VM Resizing Reports	Summarizes the VM resizing resources.
Instance Performance - Detail	Summarizes the capacity and performance details of all instances.
Region Performance - Detail	Summarizes the capacity and performance details of the selected region.
Single Instance Performance - Detail	Summarizes the capacity and performance details of the selected instance.

6

Rule Configuration Tab

The **Rule Configuration** tab of the **Cloud Manager** dashboard contains links to rules and alarms tasks that you can use to manage AWS rules and alarms.

Figure 25. Rule Configuration dashboard



To access the Rule Configuration dashboard:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **Rule Configuration** in the actions bar.

For more information, see the following topics:

- Rules view
- Enabling/Disabling rule(s)
- Adding a custom rule
- Removing custom rule(s)

Rules view

By default, the following columns are displayed in the *Rules* view:

- **Enabled**: Indicates if the rule is enabled or disabled. You can sort the list of rules by state, by clicking the Enabled column.
- **Rule**: Contains the rule name. Click the rule name to start the workflow for viewing and editing rule details.
- Fatal, Critical, and Warning thresholds (multiple-severity rules only):

- For expressions that include one registry variable, these columns contain the current value of that variable. Click the value to edit it.
- For expressions that include multiple registry variables, the column contains an icon . Clicking that icon shows the list of referenced registry variables and their values. Click a value to edit it.
- For expressions that do not include any registry variables, this column contains an icon . Clicking that icon navigates to the **Edit Rule** dashboard.
- For rule states that do not have a conditional expression defined, this column is empty.

- **Alarms**: Contains the number of alarms (multiple-severity rules only) generated by the rule. Clicking that column shows a list of alarms indicating for each alarm its severity, when the alarm was generated, and the alarm message.
- **Applies to**: Shows the object name that is applied to this custom rule.
- **Description**: Contains the rule description.

Enabling/Disabling rule(s)

The *Rule Configuration* dashboard shows a list of existing rules and a set of rule management commands at the top of the list. Use the **Enable Rule** and **Disable Rule** buttons to activate or deactivate one or multiple rules at once.

To enable a rule:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **Rule Configuration**.

   The **Rule Configuration** dashboard opens.
5. On the *Rules* list, select one or more check boxes in the left-most column, and then click **Enable Rule**.

   The *Enable Rules* dialog box opens.
6. In the *Enable Rules* dialog box, click **Yes**.

   The *Rules* list refreshes with the rules' status updated automatically.

To disable a rule:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **Rule Configuration**.

   The **Rule Configuration** dashboard opens.
5. On the *Rules* list, select one or more check boxes in the left-most column, and then click **Disable Rule**.

   The *Disable Rules* dialog box opens.

6 In the *Disable Rules* dialog box, click **Yes**.

The *Rules* list refreshes with the rules' status updated automatically.

Adding a custom rule

The *Rule Configuration* dashboard shows a list of existing rules and a set of rule management commands at the top of the list. Use the **Add Custom Rule** button to create a new rule as needed.

To customize a rule:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 Click **Rule Configuration**.

The **Rule Configuration** dashboard opens.

5 Click **Add Custom Rule** on the *Rules* table.

The *Create Custom Rule* dialog box opens.

6 In the *Create Custom Rule* dialog box, specify the following:

a Alarm Type:

a Type the name of custom rule in the *Name* field.

b Select an *Object Type*, and then select a metric from the *Metric* drop-down list. The value of *Metric* varies from the *Object Type*.

c Select either *Threshold* or *% Change*, and then specify the following values as needed.

- *Threshold*: Specify *Condition*, *Time Period*, *Severity*, and then specify whether or not fire actions if the specified data attempts are reached. The value of *Condition* cannot be negative.
- *% Change*: Specify *Condition*, *Time Period*, and *Severity Label*. The value of *Condition* cannot be negative.

b (Optional) Scope: Choose the objects to which you want to apply this rule. If no objects are selected in this step, the custom rule will apply to all objects which type is the *Object Type* specified in Step 6.

c (Optional) Notifications: Click **Add New**, then the *Edit Notification Config - Dialog* box appears. In this dialog box, type the *E-mail Address* and *Description* as needed, and then click **Add**.

7 Click **Save**.

The *Rules* table refreshes automatically to show the newly added rule.

Removing custom rule(s)

The *Rule Configuration* dashboard shows a list of existing rules and a set of rule management commands at the top of the list. Use the **Remove Custom Rule** button to delete existing custom rule(s) as needed.

To remove a custom rule:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.

4 Click **Rule Configuration**.

   The **Rule Configuration** dashboard opens.

5 Click **Remove Custom Rule** on the *Rules* table.

   The *Remove* dialog box opens.

6 Click **Yes**.

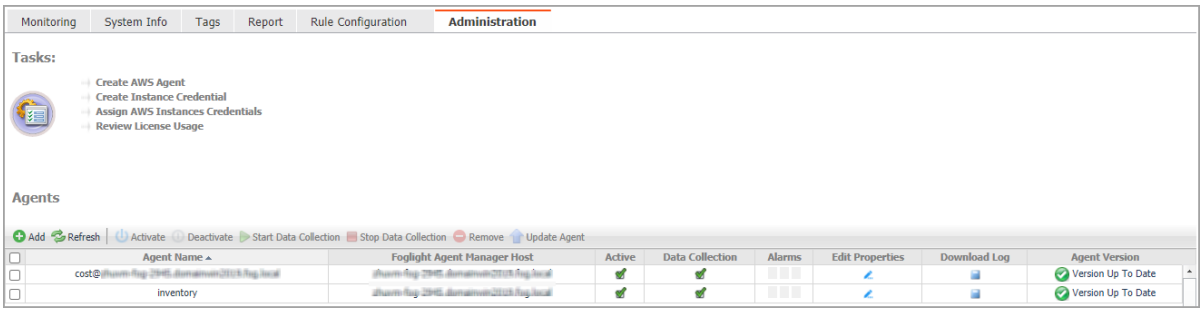
   The *Rules* table refreshes automatically and removes the selected rule.

7

Administration Tab

The **Administration** tab of the **Cloud Manager** dashboard contains links to agent administration tasks that you can use to manage AWS performance agents.

Figure 26. Administration dashboard



To access the Administration dashboard:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **Administration** in the actions bar.

For more information, see the following topics:

- Tasks view
- Agents related commands
- Creating an AWS Agent
- Editing agent properties

Tasks view

The Tasks view allows you to create an AWS agent, to create instance credentials, to assign AWS instances credentials, and to review license usage. For more information about how to create an AWS agent, refer to Creating an AWS Agent on page 12.

To create user name and password for an instance:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 Click **Administration**.

The **Administration** dashboard opens.

5 On the *Tasks* view, click **Create Instance Credential**, and then click **User Name and Password** from the prompted dialog box.

The **Add a New "User Name and Password" Credential** dialog box opens.

6 In the *Credential Properties* view, type *User Name* and *Password*, confirm the password, and then click **Next**.

7 In the *Credential Name and Lockbox* view, select a lockbox, and then click **Next**.

8 In the *Resource Mapping* view, confirm the source mapping, and then click **Next** or **Finish**.

To create a RSA key for an instance:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 Click **Administration**.

The **Administration** dashboard opens.

5 On the *Tasks* view, click **Create Instance Credential**, and then click **RSA Key** from the prompted dialog box.

The **Add a New "RSA Key" Credential** dialog box opens.

6 In the *Credential Properties* view, type *Private Key*, *Pass Phase*, and *User Name*, then click **Next**.

7 In the *Credential Name and Lockbox* view, select a lockbox, and then click **Next**.

8 In the *Resource Mapping* view, confirm the source mapping, and then click **Next** or **Finish**.

To assign credentials for AWS instances:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 Click **Administration**.

The **Administration** dashboard opens.

5 On the *Tasks* view, click **Assign AWS Instances Credentials**.

The **Credentials** dialog box opens.

6 In the **Credentials** dialog box, select a lockbox or credential, and then click the button.

The **Assign Credential** dialog box opens.

7 In the **Assign Credential** dialog box, click **Add**.

The **Choose Instance Dialog** box opens, select an instance, and then click **Select**.

8 The **Choose Instance Dialog** box closes, and the selected instance appears on the *EC2 Instances* table. Click **save**.

To review license usage:

1 Log in to the Foglight browser interface.

2 Ensure that the navigation panel is open.

To open the navigation panel, click the right-facing arrow on the left.

3 On the navigation panel, under *Homes*, click **Cloud Manager**.

The **Cloud Manager** dashboard opens.

4 Click **Administration**.

The **Administration** dashboard opens.

5 On the *Tasks* view, click **Review License Usage**.

The **Review License Usage** dialog box opens.

6 Click **AWS** in the **Review License Usage** dialog box to review the current AWS license information.

The *AWS license* table shows the *Account*, *Monitoring Agent*, and *Monitored Instance Count* of your license.

7 Click the number in the *Monitored Instance Count* column.

The **Instances** dialog box opens and shows the detailed information about all monitored instances.

If the number of monitored instance goes beyond your valid license, the following message will shows on the **Cloud Manager** dashboard: "*Caution: Foglight Hybrid Cloud Manager is over-deployed by <number> monitored virtual machines. Please contact Quest to purchase additional licenses.*"

Agents related commands

The **Administration** dashboard shows a list of existing agent instances and a set of agent management commands at the top of the list. Use it to verify that your agents are collecting data from the monitored environment.

The following commands are available:

- **Add:** Starts a workflow for creating new agent instances. For more information, see Creating an AWS Agent on page 12.
- **Refresh:** Refreshes the list of agent instances and their states.
- **Activate:** Activates one or more selected agent instances. Activating an agent instance starts the agent process on the machine on which the agent is installed.
- **Deactivate:** Deactivates one or more selected agent instances. Deactivating an agent stops the agent process on the machine on which the agent is installed.
- **Start Data Collection:** Starts the data collection for one or more selected agent instances. Starting an agent's data collection causes the agent to begin monitoring the AWS accounts and to send the collected metrics back to the Management Server.
- **Stop Data Collection:** Stops the data collection for one or more selected agent instances. Stopping an agent's data collection causes the agent to stop monitoring the AWS accounts.
- **Edit Properties:** Starts a workflow for editing the properties of one or more selected agent instances. Each agent comes with a set of properties that it uses to configure its correct running state. Editing agent properties on page 49.
- **Remove:** Deletes the selected agent instance.

- **Update Agent:** Updates the agent package to the latest version.

  IMPORTANT: Updating the agent package using this command generates the previously existing credentials. However, if you update the agent package by re-deploying its .gar file through the Agent Status page, the credentials need to be re-created. To do that, select an agent instance, click **Edit Properties**, and configure the required credentials on the **Credentials** tab of the **Edit Tab Manager** dialog box.

To perform any of the available commands, select one or more check boxes in the left-most column and click the appropriate button. For example, to start an agent's data collection, select the check box in the agent row and click **Start Data Collection**.

Editing agent properties

AWS Agents collect data from your AWS infrastructure and send it to the Management Server. The agents keep track of resource utilization metrics and alerts you when certain pre-defined thresholds are reached.

Default versions of these properties are installed with Foglight. However, you can edit the default agent properties, configure the agent properties that apply only to a specific agent instance, and create edited clones of shareable properties that are used by a subset of certain agent type.

To edit the AWS Performance Agent properties:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

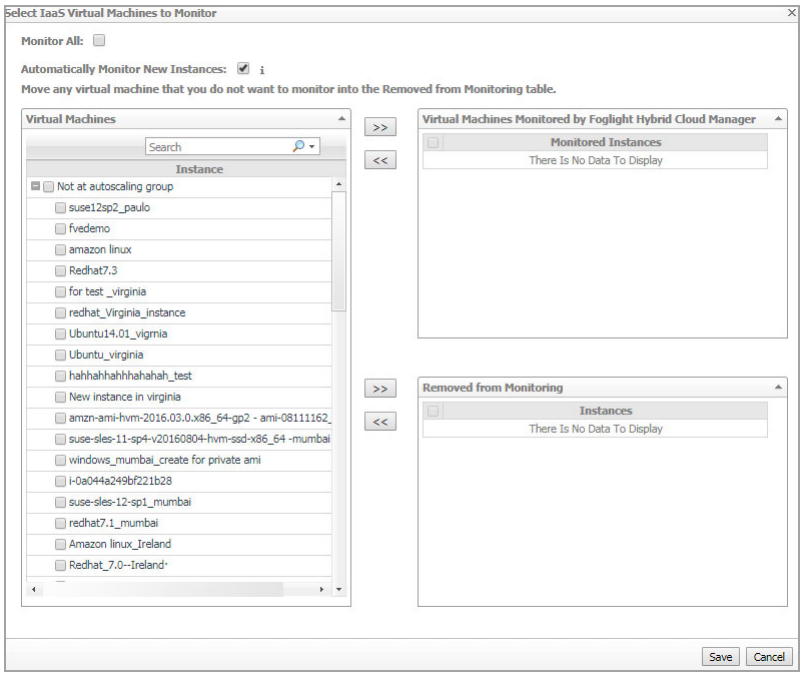
   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   Cloud Manager dashboard opens.
4. Click **Administration**.

   The **Administration** dashboard opens.
5. Select the instance of the AWS Agent properties that you want to modify, and then click **Edit Properties.**
6. In the **Edit Properties** dialog box, edit the following properties, as needed.
   - *Account Alias*: The display name of this account.
   - *Access Key ID*: The access key retrieved in Getting authentication information through console on page 11.
   - *Secret Access Key*: The secret access key retrieved in Getting authentication information through console on page 11.
   - *Collect Memory Metric*: Select this option to enable the collection of instance memory metrics. The default value is disabled.
   - *Collect Linux Volume Utilization*: Select this option to enable the collection of Linux volume utilization. The default value is disabled.
   - *Specify an agent name (Optional)*: Specify the name of agent.
   - *Configure regions to be monitored (Optional)*: Select AWS regions for monitoring. All regions will be monitored if this field is not configured.
   - *Select Virtual Machines to Monitor*: Specify to monitor all virtual machines or only monitor specified instance.
     - *If Monitor All is selected*: By monitoring all virtual machines any virtual machine that is running in the monitored cloud will be monitored 24x7 consuming a monitored virtual machine license. Every virtual machine that is monitored will count against the purchased

license pool. Any Monitored Virtual Machine that is above the purchased license limit will require an additional Foglight Hybrid Cloud Manager per Monitored Virtual Machine license.

- *If Monitor All is not selected*: The following view appears on the bottom of the **Selected IaaS Virtual Machines to Monitor** dialog box.



  - If *Automatically Monitor New Instances* is selected, select instances that you do not want to monitor, and then click >> to move selected instances to the *Removed from Monitoring* table.
  - If *Automatically Monitor New Instances* is not selected, select instances that you want to monitor, and then click >> to move selected instances to the *Virtual Machines Monitored by Foglight Hybrid Cloud Manager* table.
  - If the *Removed from Monitoring* and *Virtual Machines Monitored by Foglight Hybrid Cloud Manager* tables are empty, and *Automatically Monitor New Instances* is not selected, the AWS agent will not collect any instance data.

- *Configure Account Cost to Monitor*:

  Configure the Cost Metrics collection. Collections will start only after the AWS Cost and Usage Report are created on the AWS Console. See To create an AWS Cost and Usage Report.

  - *Collect Cost Metrics:* Select the check box to enable and configure the cost metrics collection. Collections will start only after the AWS Cost and Usage Report are created on the AWS Console. See To create an AWS Cost and Usage Report.
    - *Configure Monitor Account:* Click **Configure** to select the accounts for which costs should be monitored**.**

      By default, **Collect All Account Cost** is selected. This will collect consolidated billing information for all accounts in a single organization. To manually select accounts for cost collection, clear **Collect All Account Cost**.
    - *Select Account:* When **Collect All Account Cost** is cleared, a list of AWS accounts in your organization will be displayed. Note that accounts will only be displayed after a successful data collection. In the **AWS Account** table, select the accounts to monitor and click >> to add the accounts to the **Target AWS** account table.

      Adding accounts: If the desired accounts do not appear in the accounts listed in the **AWS Account** table, you can manually add the account by clicking **Add** and

supplying the **Account ID (**See To get Account ID (12-digit number) to get this value) and **Account Name.**

Note: Accounts added to the AWS Account table will not be saved unless they are moved to the Target AWS table.

- *Import/Export accounts:* In addition to manually adding accounts, they can be imported (from a CSV file) to either the **AWS Account** or **Target AWS Account** table. Accounts can also be exported from the **Target AWS Account** table.

  The CSV file should contain two columns :**Account ID(12-bit Numbers)** and **Account Alias Name.** See To get Account ID (12-digit number) for more information.

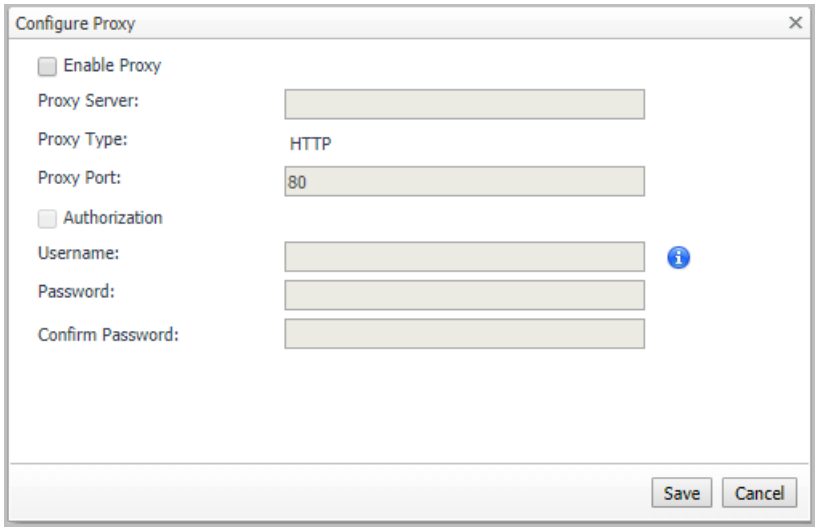
  Note: Accounts imported to the AWS Account table will not be saved unless they are moved to the Target AWS table.

- Click **Save** to save changes.

- *S3 Bucket for Cost and Usage Report*: Enter the name of your S3 bucket according to the AWS Cost and Usage Report setting. See To create an AWS Cost and Usage Report to get this value.
- *S3 Bucket Region for Cost and Usage Report*: Select the region of your S3 bucket according to the AWS Cost and Usage Report setting. See To create an AWS Cost and Usage Report to get this value.
- *Cost and Usage Report Name:* Enter the name of your AWS Cost and Usage report. See To create an AWS Cost and Usage Report to get this value.
- *Cost and Usage Report Path:* Enter the Report path prefix according to your Report setting. The value of Cost and Usage Report Path will be blank, if you don't set the Report path prefix in AWS. See To create an AWS Cost and Usage Report to get this value.

- *Configure Proxy (Optional)*:

Configure the proxy setting when the Agent Host requires a proxy connection to the Internet.



a Select the *Enable Proxy* check box to enable the proxy settings.

b Input the host name or IP address for the *Proxy Server* and input the Proxy Port number.

c If the proxy requires an authorization, select the *Authorization* check box, and input the Username and Password.

NOTE: In FIPS-compliant mode, if proxy settings are configured, you need to import the proxy server application root certificate into FMS KeyStore and FgLAM. For more information, see Managing certificates.

7 Click **Save**. The **Edit Properties** dialog box closes and the list of agent instances automatically refreshes in the display area.

Managing certificates

Syntax Conventions

In order to successfully make use of the Foglight commands in your monitoring environment, review the syntax conventions before getting started. The syntax conventions are as follows:

- Generic examples follow the UNIX path structure that uses forward slashes '/' to separate directories.
- Platform-specific examples follow standard platform conventions. For example, UNIX-specific examples use forward slashes '/' as directory delimiters, while Windows examples use backslashes '\'.
- *<foglight_home>* is a placeholder that represents the path to the Foglight Management Server installation.
- *<foglight_agent_mgr_home>* is a placeholder that represents the path to the Foglight Agent Manager installation. This can be the location of the Foglight Agent Manager installation on a monitored host, or the home directory of the Foglight Agent Manager that comes embedded with the Foglight Management Server. For example:

  Path to the Foglight Agent Manager installation on a monitored host (Windows):

  C:\Quest\Foglight_Agent_Manager

  Path to the embedded Foglight Agent Manager installation (Windows):

  C:\Quest\Foglight\fglam
- Unless otherwise specified, Foglight commands are case-sensitive.

Managing certificates for FglAM

Foglight Evolve agents use Foglight Agent Manager (FglAM) to manage certificates for SSL encryption connection.

Prerequisite

All the certificate-related command line options require that FglAM be **up and running**.

Add a certificate

```
bin/fglam --add-certificate "user alias 1"=/path/to/certificate/file
```

- Validate the certificate and ensure the following:
  - It is not expired.
  - It is an X.509 format.
  - FglAM requires the Base64 format. To verify if the certificate file is encoded with Base64, open the certificate with a notepad and the certificate should be similar to the following example:
    `-----BEGIN CERTIFICATE-----`

```
XXXXXXXX=
-----END CERTIFICATE-----
```

NOTE: If the certificate is not Base64 format, use openssl command to convert the certificate file into a Base64 file. Use either of the following commands depending on the source form:
`openssl x509 -inform DER -in xxx.cer -out xxx.crt`
or
`openssl x509 -inform PEM -in xxx.cer -out xxx.crt`

- The `alias` is required and is used in the list and delete operations to refer to the certificate. It can be anything.

List installed certificates

`bin/fglam --list-certificates`

Print out a list of certificates and the aliases that refer to them.

Refer to the example output below:

```
List of installed certificates:
  Alias                Certificate Info
  -----                ----------------
  user alias 1        XXXX
```

Delete a certificate

Remove a certificate referred to by an `alias`.

`bin/fglam --delete-certificate "user alias 1"`

A full example for managing certificate for FglAM

- Add an example certificate into FglAM certificate store

  ```
  C:\Quest\Foglight\fglam\bin>fglam.exe --add-certificate "Evolve-test"="D:/Evolve-test.crt"
  …
  2020-02-27 16:31:01.000 INFO  [native] Certificate added: Certificate from
    D:\Evolve-test.crt added as Evolve-test
  ```

- List the example certificate in the FglAM certificate store

  ```
  C:\Quest\Foglight\fglam\bin>fglam.exe --list-certificate
  …
    Alias                       Certificate
    -----                       -----------
    Evolve-test                         Issuer:
                                  CN: XXX
  ```

- Delete the example certificate from the FglAM certificate store

  ```
  C:\Quest\Foglight\fglam\bin>fglam.exe --delete-certificate "Evolve-test"
  …
  2020-02-27 16:28:21.000 INFO  [native] Certificate deleted: Certificate
  ```

```
Evolve-test deleted
```

Managing certificates for FMS in FIPS-compliant mode

Use the keytool utility shipped with Foglight to create, import, or export certificates. This utility can be found at: *<foglight_home>\jre\bin\keytool*.

The KeyStore Foglight used in FIPS-compliant mode is located at: *<foglight_home>/config/security/trust.fips.keystore* (default password: `nitrogen`)

Add a certificate in FIPS-compliant mode

Use the keytool command in FMS JRE located in *<foglight>/jre/bin.*

```
keytool -import -trustcacerts -alias "<alias>" -file "<certificate path>" -keystore
"<Foglight_home>/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen
```

- Validate the certificate and ensure the following:
  - It is not expired.
  - It is an X.509 format.
- Change the following before executing the command
  - `<alias>`: The alias is required and is used in the list and delete operations to refer to the certificate. It can be anything.
  - `<Foglight_home>`: The folder path where Foglight is installed.
  - `<certificate path>`: Your custom certificate path.

List installed certificates

```
keytool -list -keystore "<Foglight_home>/config/security/trust.fips.keystore" -
deststoretype BCFKS -provider
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen
```

Prints out a list of certificates and the aliases that refer to them.

Refer to the example output below:

```
Keystore type: BCFKS

Keystore provider: BCFIPS

Your keystore contains 151 entries

camerfirmachambersignca [jdk], Dec 18, 2019, trustedCertEntry,

Certificate fingerprint (SHA1):
4A:BD:EE:EC:95:0D:35:9C:89:AE:C7:52:A1:2C:5B:29:F6:D6:AA:0C

entrust2048ca [jdk], Dec 18, 2019, trustedCertEntry

…
```

Delete a certificate

Remove a certificate referred to by an `alias`.

```
keytool -delete -alias <alias> -keystore
"<Foglight_home>/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"<Foglight_home>/server/core/bc-fips.jar" -storepass nitrogen
```

A full example for managing certificate for FMS in FIPS-compliant mode

Add example certificate into FMS certificate store in FIPS-compliant mode

```
C:\Quest\Foglight\jre\bin>keytool -import -trustcacerts -alias "Evolve-Test" -file
"D:/Evolve-test.crt" -keystore
"C:/Quest/Foglight/config/security/trust.fips.keystore" -deststoretype BCFKS -
provider org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath
"C:/Quest/Foglight/server/core/bc-fips.jar" -storepass nitrogen

Owner: CN=CA, DC=ca, DC=local

Issuer: CN=CA, DC=ca, DC=local

Serial number: xxxx

Valid from: Sun Jan 06 23:07:06 CST 2019 until: Wed Apr 06 23:07:06 CST 2022

Certificate fingerprints:

...


Extensions:

...

Trust this certificate? [no]:  yes

Certificate was added to keystore
```

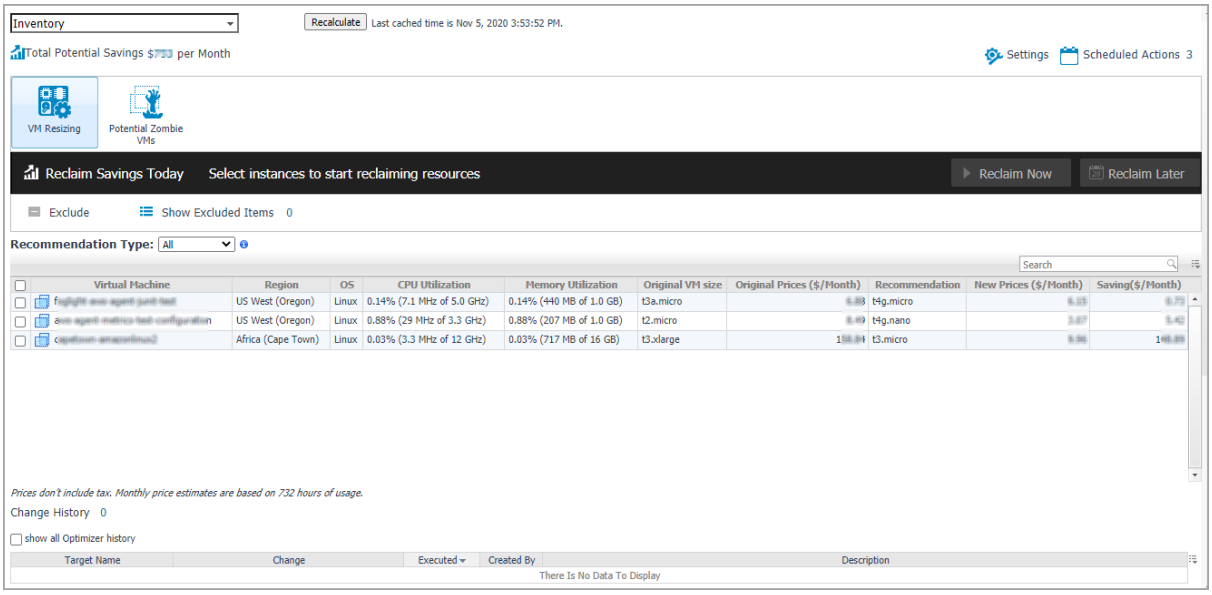
8

Optimizer Tab

NOTE: If your FMS host doesn't have Internet connection, **VM Resizing** recommendations will not work properly. Ensure that the proxy is enabled and the settings are configured under **Administration** > **Proxy Configuration**.

Click **Optimizer** on the top of the **Cloud Manager** dashboard to navigate to the **Optimizer** tab.

Figure 27. Optimizer tab



To access the Optimizer tab:

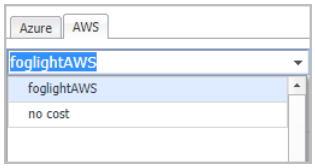
1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

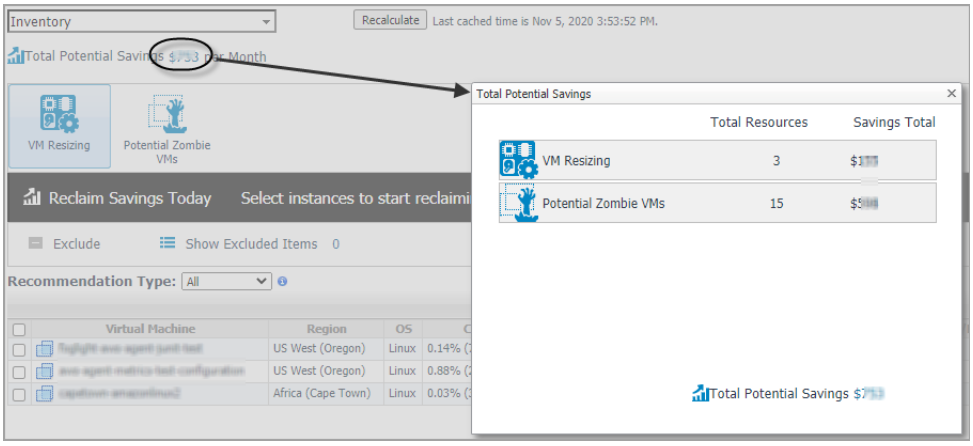
   The **Cloud Manager** dashboard opens.
4. Click **Optimizer**. The **Optimizer** tab opens on the bottom of **Cloud Manager** dashboard.
5. Click **AWS**. The *Optimizer - AWS* view opens.

The *Optimizer - AWS* view includes the following elements:

- **Group selector**: The group selector is located at the top of the *Optimizer - AWS* view and allows you to select the AWS environment that you want to optimize.



- **Recalculate**: Click the button to recalculate the data. Click **Recalculate** on the *Recalculate Confirmation* dialog box to start recalculating.
- **Total Potential Savings**. Shows the potential savings per month. Click the savings and a *Total Potential Savings* dialog box opens. It displays the total resources and total savings for VM Resizing and Potential Zombie VMs.



- **Settings**. The **Settings** dialog box is used to change the time period and properties that are used for calculation. For more information, see Settings on page 58.
- **Scheduled Actions**. The **Scheduled Actions** dialog shows the list of operations scheduled to be run at a particular time in the future, and allows you to edit or remove any scheduled actions. To view only the actions specific to Foglight Resource Optimizer, select the ***show only Optimizer actions*** checkbox. When the checkbox is not selected, the dialog shows all actions scheduled for your virtual environment.
- **VM Resizing**. Shows instance name, utilization, and recommendations for both CPU & memory resources.
- **Potential Zombie VMs**. Shows instance name, regions, CPU, memory, disk throughput, and network of the zombie virtual machines based on calculation settings.

  NOTE: Both EBS-backed and Instance-store root device type can be calculated for VM resizing and zombie VM recommendation. However, only the EBS-backed device type resource can be reclaimed.

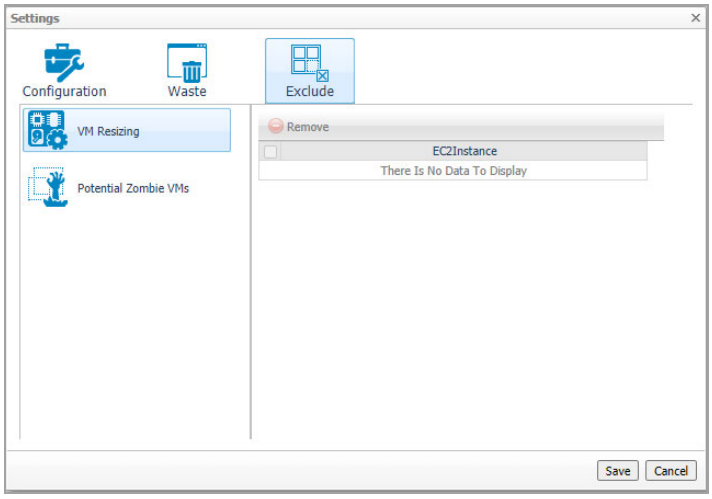
- **Reclaiming Savings** bar. The **Reclaiming Savings** bar enables the system administrator to select instances from the list and review the resources that can be reclaimed.
  - To reclaim the resources wasted for a selected instance, click **Reclaim Now**.
  - To schedule reclaiming the resources wasted for a selected instance, click **Reclaim Later**.

  NOTE: To use the Optimizer Reclaim actions, the minimum application privileges are required. For more information, see Minimum application privileges on page 7.

- **Exclude**. After selecting an instances either in the VM Resizing or Potential Zombie VMs instance table, click **Exclude** to remove the selected instances from calculation.

  NOTE: The **Reclaim Now** and **Reclaim Later** buttons and the **Exclude** link are enabled only after selecting an instance from the table.

- **Show Excluded Items**. Click the **Show Excluded Items** button or ***Settings*** > ***Excluded*** tab to show the instances that have been excluded from calculation.



- **Recommendation Type**: Include three options: *All*, *Executable*, and *Inexecutable*. Use to filter the resources that can be reclaimed or review the resources that cannot be reclaimed.
- **Change History** view. The **Change History** embedded view shows the changes that have been implemented in the environment during the **History Period [x] Day(s)**, the object that was affected, and the result of the operation.

  To view the change history of all Optimizer tabs, select the ***show all Optimizer history*** checkbox. When the checkbox is not selected, the view shows only the change history for the selected Optimizer tab.

  The number at the top of the view indicates the total number of changes executed for the selected VM component, during the **History Period [x] Day(s)**.

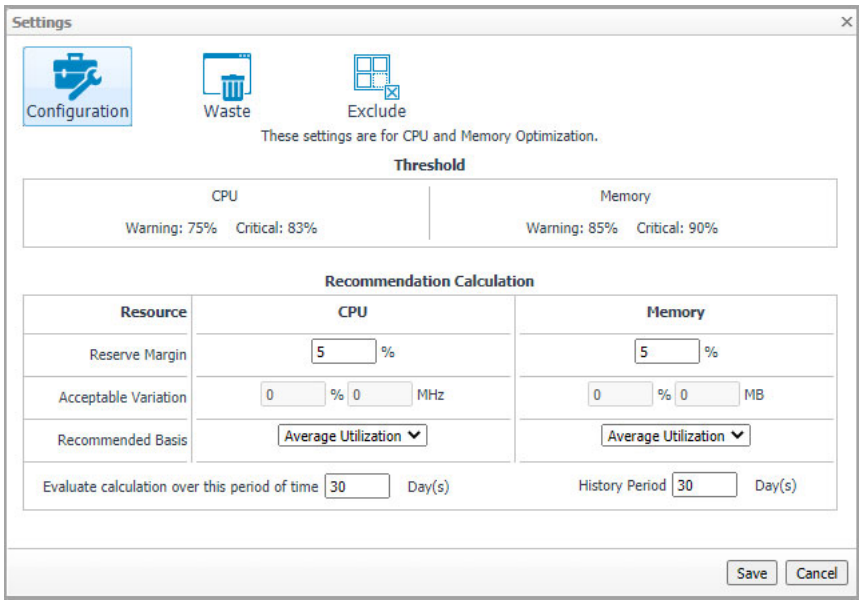
  - **Target Name**. Virtual machine that was affected by the change.
  - **Change**. Type of change.
  - **Executed**. Date and time when the change was executed.
  - **Created By**. User who scheduled the change.
  - **Description**. Operation result: *Completed*, *In progress*, or *Failed* (and an explanation why the job has failed).

Settings

Use the **Settings** menu to define the default optimization settings for your environment. The **Settings** Dialog box provides information about the following components:

- Configuration tab
- Waste tab
- Excluded tab

Configuration tab

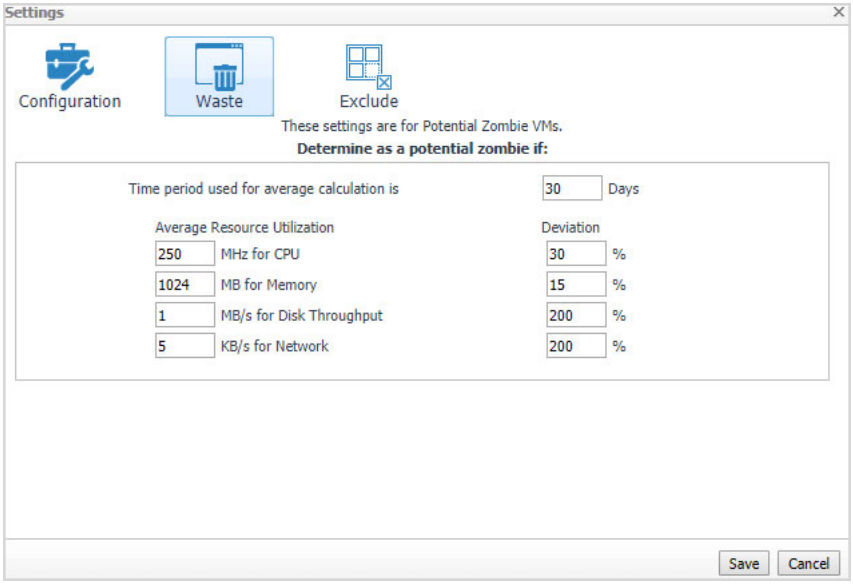


The **Configuration** tab provides the recommended settings for CPU and memory optimization.

- **Thresholds**. Provides the values of a resource metric that define the Warning and Critical levels (for CPU and memory).
- **Recommendation Calculation** area. Allows you to define the following parameters for optimizing the CPU and memory resources in your environment:
  - **Reserve Margin [x]%**. This parameter is used for calculating the Evaluation Result, which is needed for making recommendations. The Recommendation Reserve Margin percentage is the percentage above the recommended basis, reserved for unexpected increases in utilization.
  - **Acceptable Variation**. Don't use at AWS resource calculation now.
  - **Recommended Basis**. Use this list to select the *Recommended Basis* to be used for calculating the Evaluation Result. Currently just support Average Utilization.
  - **Evaluate calculation over this period of time [x] Day(s)**. Defines the time interval during which the right-sizing calculation is performed.
  - **History Period [x] Day(s)**. The Change History view displays the changes for the time interval defined here.

To save any changes made to the **Configuration** settings, click **Save** at the bottom of the tab.

Waste tab



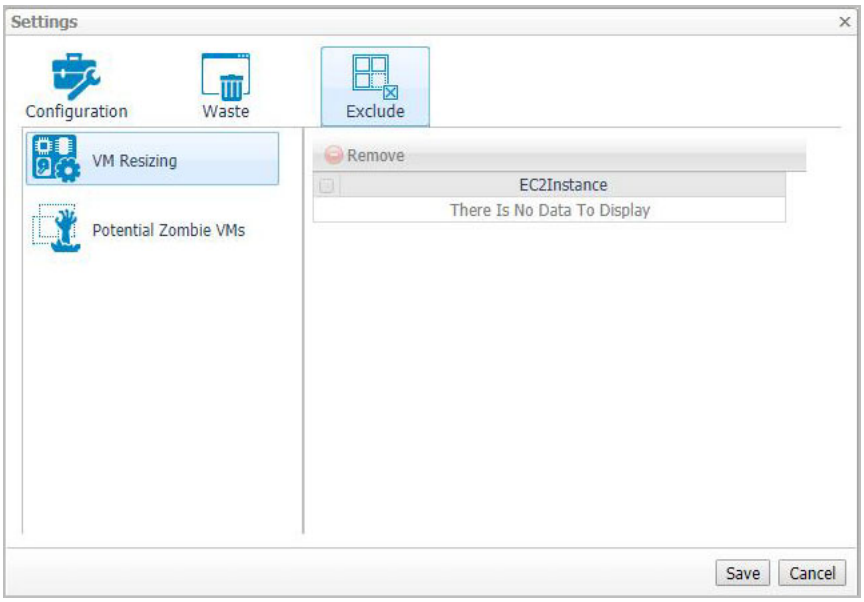
The **Waste** tab allows you to configure the settings for determining resources wasted in your environment. These include powered-off instances, and potential zombie VMs:

- **Determine as a potential zombie if area**: A VM is considered a zombie VM if the following five settings are met:
  - **Time period used for average calculation is [x] Days**. Defines when a resource is considered a zombie VM, by looking at the period used for average calculations.
  - **Average Resource Utilization-Deviation**. Defines when a resource is considered a zombie VM, by looking at the CPU, memory, disk throughput, and network utilization values.

    TIP: Deviation is the maximum deviation from the average resource utilization that is allowed for a VM considered to be a zombie.

To save any changes made to the **Waste** settings, click **Save** at the bottom of the tab.

Excluded tab



The **Excluded** tab allows you to remove an instance from the list of excluded objects. The **Excluded** tab includes the following information:

- On the left side, a navigation tree, that allows you to select the VM component category.
- On the right side, the list of instances excluded from the selected VM category.

To remove instances from the list of **Excluded** objects, select the check boxes for these instances and click **Remove**. To save any changes made to the **Excluded** settings, click **Save** at the bottom of the tab.

The **Excluded** tab can also be accesses by clicking **Show Excluded Items** on **Optimizer**.

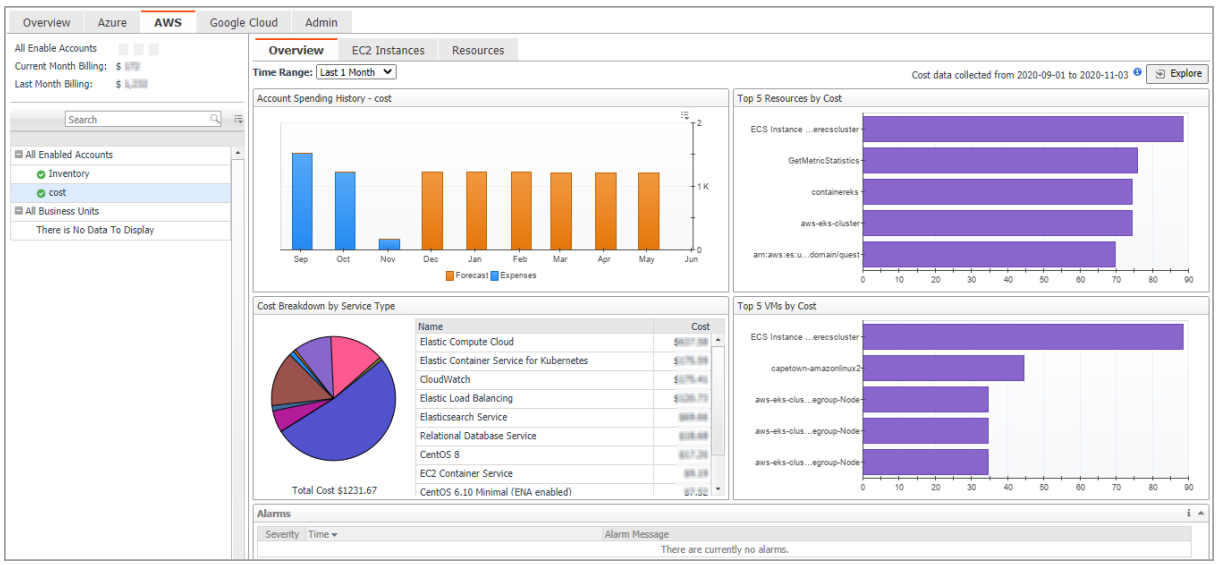
9

Cost Tab

Click **Cost** on the top of the **Cloud Manager** dashboard to navigate to the **Cost** tab.

NOTE: Ensure that you have configured the cost metrics for account through the **Agent Properties** dialog box; otherwise there will have no data displayed on this tab. For more information about how to configure cost metrics, refer to the Configure Account Cost to Monitor: on page 50.

Figure 28. Cost tab



To access the Cost tab:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **Cost**. The **Cost** tab opens on the bottom of **Cloud Manager** dashboard.
5. Click **AWS**.

Cost - Overview

The *Cost-Overview* includes the following elements:

- **Cost Summary**: Displays the Total Month-to-date cost, and cost by Azure, AWS, and Google Cloud platforms.

- **Cost Overview**: A stacked bar chart to display the Month-to-date Expenses and Forecast by Azure, AWS, and Google Cloud platforms.

NOTE: The Month-to-date (MTD) indicates a period starting from the beginning of the current month till the end of the current date.

- **Infrastructure**: Displays an Infrastructure resource table across clouds.
  - Accounts Configured: The number of Azure subscription, AWS Accounts, or Google Cloud Billing Accounts.
  - Total VMs: The total number of VMs running in the Cloud platform.
- **Top 5 Business Units by Cost**: Aggregates the total cost for Business Units after users assign the AWS accounts, Azure Subscriptions, or Google Cloud Billing Accounts to a BU under **Cost** > **Admin**.
- **Cost Breakdown by Platforms**: Displays the Month-to-date cost by Azure, AWS, and Google Cloud platforms.

Cost - AWS view

The *Cost - AWS* view includes the following elements:

- Overview of all enabled Accounts cost: Lists the enabled accounts, billing of the current month, and billing of the last month.
- Object tree view: Lists the enabled Accounts and business units.
- Time Range Selector: Lists the time range for billing. The time bar of the Management Server does not take effects on the *Cost* dashboard.
- All Enabled Accounts Spending History/Top 5 Accounts by cost/Spending Breakdown: These three views will display the relevant cost information if you select *All Enabled Accounts* or *All Business Units* from the object tree view.
- Account Spending History/Top 5 Resources by Cost/Cost Breakdown By Service Type/Top 5 VMs by Cost: These four views will display the cost information of the selected account or business unit.
- Alarms: Lists all alarms against the selected account or business unit.
- Select Account displays the cost overview, EC2 Instances in account, and Resource cost overview.

Cost - Admin view

The Cost - Admin view includes the following:

- AWS Accounts tab: Displays the overview of all accounts, including the account name, business unit, spending, monthly budget, last month billing, current month billing, and next month projection.
  - Set Monthly Budget: Updates monthly budget for selected account.
  - Assign Business Unit: Assigns the select accounts to a Business Unit.
  - Remove from Business Units: Exits the selected business units.
- Business Units tab: Lists business units name, location, organization, and accounts.
  - Add Business Units: Creates a business unit, specifies Business Unit name, description, location, longitude, latitude, and assigns to a new organization or existing organization.
  - Delete Business Units: Deletes selected business units.
  - Assign Organization: Select the organization from the list for selected business units.

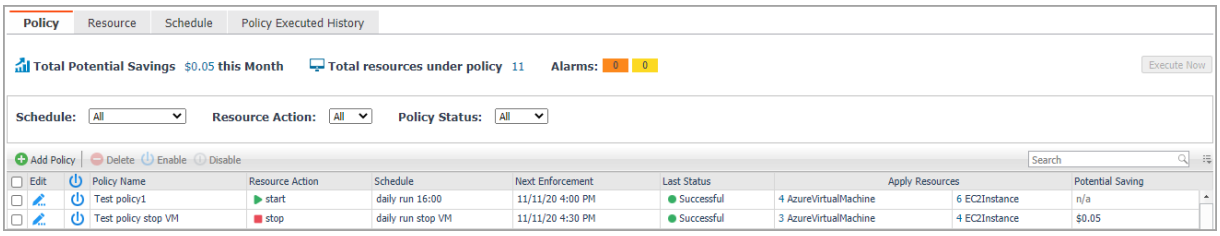
10

Policy Management Tab

Policy Management enables user to start or stop their resources by schedule. Currently, only the resource type of VM is supported.

NOTE: To use the Policy Management feature, a Foglight Evolve Cloud or Flex license is required. Contact Quest Support to purchase a license.

Figure 29. Policy Management tab



To access the Policy Management tab:

1. Log in to the Foglight browser interface.
2. Ensure that the navigation panel is open.

   To open the navigation panel, click the right-facing arrow on the left.
3. On the navigation panel, under *Homes*, click **Cloud Manager**.

   The **Cloud Manager** dashboard opens.
4. Click **Policy Management**. The **Policy Management** tab opens on the bottom of **Cloud Manager** dashboard.

Policy view

The *Policy* view includes the following elements:

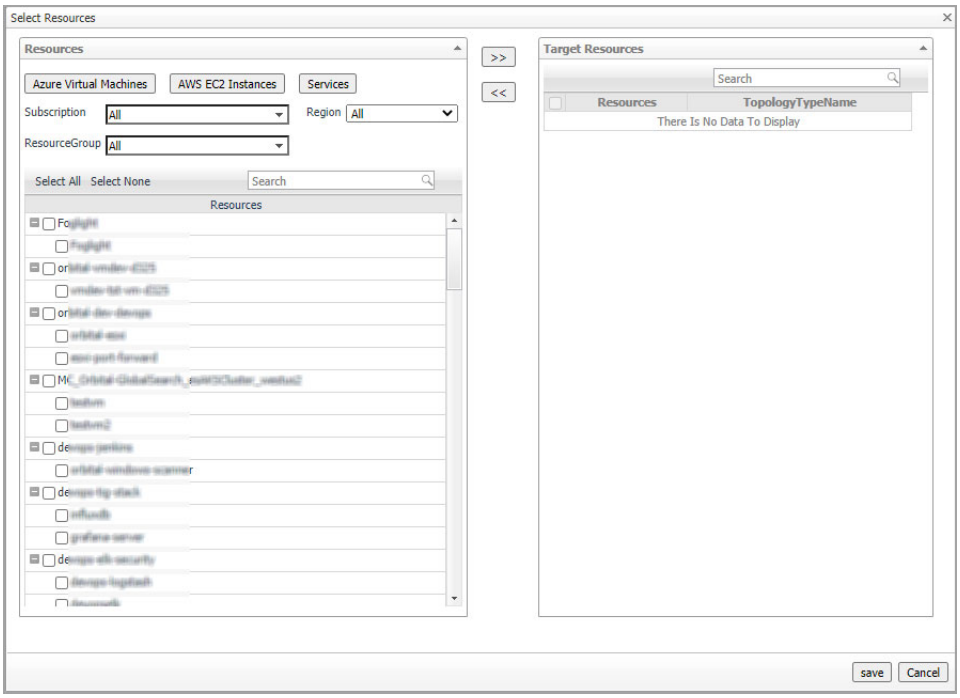
- **Total Potential Savings**: Shows the total potential savings of this month under the policies. The potential savings are calculated by the total hours the VMs has been stopped by the policy multiply the unit price of each VM.

  NOTE: The potential saving would be automatically recalculated every 30 minutes.
- **Total resources under policy**: Shows the total number of resources managed under the policies. For a detailed resource list, refer to Resource view on page 66.
- **Alarms**: Shows the number of alarms (multiple-severity rules only) generated by the policy. Clicking the numbers, an alarm list will be displayed. The list shows the severity of each alarm, when the alarm was generated, and the detailed alarm message.
- **Execute Now**: Click **Execute Now** to execute the selected policy immediately.

- Filters. Including by **Schedule**, by **Resource Action** (Start or Stop), and by **Policy Status** (Enable or Disable).
- **Add Policy**. Click **Add Policy** and an *Add Policy* dialog box appears. It includes the following elements:
  - *Policy Name*: Specify a policy name.
  - *Description*: Add descriptions about the policy.
  - *Enable*: Select the checkbox to enable the policy.

    NOTE: Only the enabled policies will be executed by schedule.

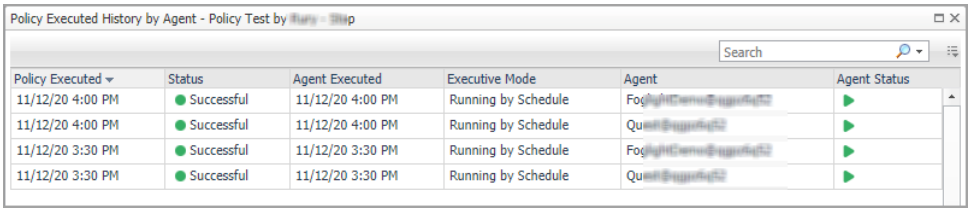
  - *Action*: Select an action for the policy. You can either start a VM or stop a VM.
  - *Schedule*: Select a schedule. You can either assign the policy to a new schedule or assign the policy to an existing schedule.
  - *Apply Resources*: Select the resources you would like to apply the policy. Click **Apply Resources** and a *Select Resources* dialog box appears.



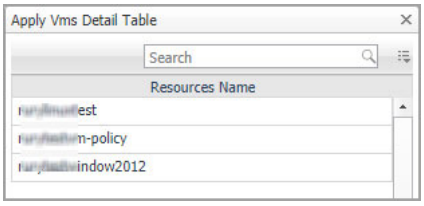
    Select Resources by types:

    - **Azure Virtual Machines**: A tree table lists VMs by Resource Groups.
    - **AWS EC2 Instances**: A Tree table lists Instances by Auto scaling group.
    - **Services**: Lists the service from ***Dashboards*** > ***Services*** > ***Service Builder***.
  - *Email Notification*: Enter e-mail addresses to notify the users when the policy is executed.
  - *Process Service Dependencies*: If applying resources by a service and the resources are collected by the same agent, the VMs under the child service will be executed first.
- A policy list table. The table includes the following elements:
  - Edit: Click the icon and an *Edit Policy dialog* box appears. Update the policy and save the changes.
  - Enable: Click the icon to enable a policy.
  - *Policy Name*: Lists the name of the policy.
  - *Resource Action*: Shows the action status of the policy, including **start** and **stop**.
  - *Schedule*: Shows the schedule of the policy.

- *Next Enforcement*: Shows the time when the policy will be executed again.
- *Last Status*: Shows the last status after the policy was executed. Click the status and a *Policy Executed History by Agent* dialog box will appear.



- *Apply Resources*: Shows the selected resources by object type. Click the resources and an *Apply VMs Detail Table* will appear.

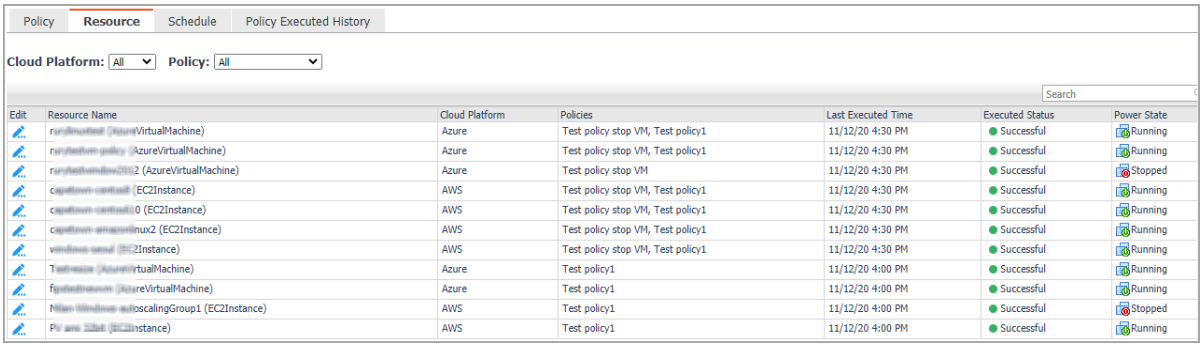


- *Potential Saving*: Shows the total potential savings of this month under the policy. The potential savings are calculated by the total hours the VMs stopped by the policy multiply the unit price of each VM.

Resource view

The *Resource* view shows all the VMs which are managed by the polices. Users can add resources to polices or remove resources from polices.

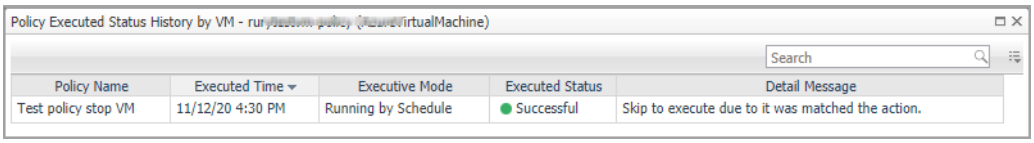
Figure 30. Resource view



The *Resource* view includes the following elements:

- Filters. By **Cloud Platform** and by **Policy**.
- A resources table. Shows a list of resources managed by the policies. The table includes the following elements:
  - Edit: Click the icon and an *Edit VM* dialog box will appear.
  - *Resource Name*: Shows the name of the resource.
  - *Cloud Platform*: Shows the cloud platform the resource belongs to.
  - *Policies*: Shows the policy that manages the resource.

- *Last Executed Time*: Shows the last time when the policy was executed. Click the time and a *Policy Executed History by VM* dialog box will appear.
- *Executed Status*: Shows the last status after the policy was executed. Click the status and a *Policy Executed History by VM* dialog box will appear.

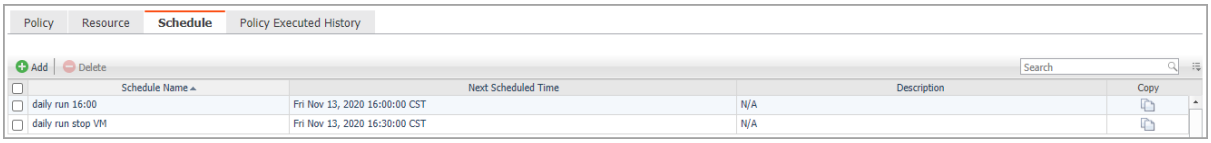


- *Power State*: Shows the power status of the resource.

Schedule view

The Schedule view enables users to create, edit, delete, or copy a schedule.

Figure 31. Schedule view



To create a new schedule, do either of the following:

- Click **Add** and a *Create Schedule* dialog box appears.
  1. *Occurrence*: Select the start date and start time and click **Next**.
  2. *Recurrence*: Select the recurrence and click **Next**.
     a. Specify the Recurrence Pattern according to the screen prompt. Click **Next**. For detailed information of the Recurrence Pattern, see Recurrence Pattern on page 68.
     b. Choose *Never Stop* or specify an *End Time*. Click **Next**.
  3. *Summary*: Specify a name for the schedule and descriptions for the schedule. Click **Finish**.
- Click **Copy** and a *Copy [Schedule name]* dialog box appears. Edit the schedule name and description. Click **OK**.

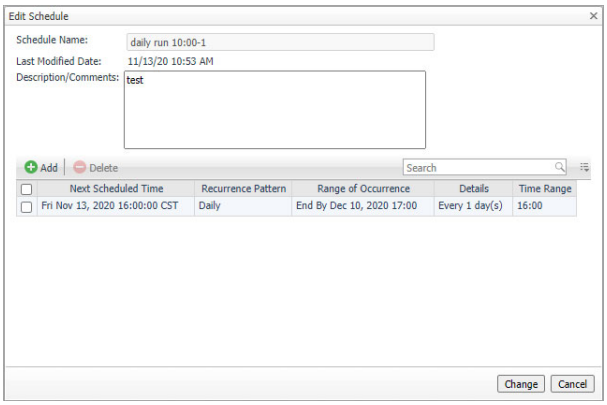
The schedule list refreshes and the newly-created schedule will be displayed in the list.

To delete a schedule, do the following:

1. Select a schedule from the schedule list and click **Delete**.
2. A *Delete Schedules Confirmation* dialog box appears.
3. Click **OK**.
4. The schedule list refreshes and the schedule will be removed from the schedule list.

To edit a schedule, do the following:

1. Click the schedule you want to edit and an *Edit Schedule* dialog box appears.



2 Click the schedule and an *Edit Schedule Item* dialog box appears.

3 Edit the *Occurrence*, *Recurrence*, and *Summary* if necessary and click **Finish**.

Recurrence Pattern

Table 50. Description of the Recurrence Pattern

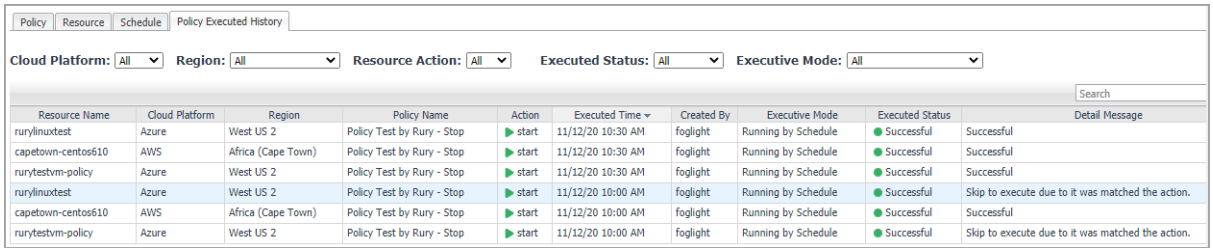
Pattern Name	Pattern Description	Pattern Settings
Once	Starts at a specified date and time, for a specified duration, and ends at a defined end date and time.	N/A
Interval	Starts at a specified time and date for a certain duration, repeats at specified time periods, with or without a defined end date and time.	Specify *Every xx* and select from *Days, Hours, Minutes,* or *Seconds*.
Daily	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of days, with or without a defined end date and time.	Specify *Every xx days*.
Weekly	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of weeks on one or more days of the week, with or without a defined end date and time.	Specify *Every xx week (s)* and select the weekdays.
Monthly	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of months on one or more days of the month, with or without a defined end date and time.	Select by *Day* or *Week*. Specify *Day xx of Every xx month(s)*.
Yearly	Starts at a specified time and date, runs for a whole day or a fraction of a day, repeats at a regular interval of years on one or more days of the year, with or without a defined end date and time.	Select by *Day of Month* or *Week of Month*. Specify the date and select the month.

IMPORTANT: Schedules consisting of multiple scheduled items must include a relevant start time. By default, the start time is the day the schedule is created. The start time of each schedule item must be specified to reflect the first run of the scheduled item.

Policy Executed History view

The **Policy Executed History** view shows the detailed history records of the executed policy by each Resource.

Figure 32. Policy Executed History view

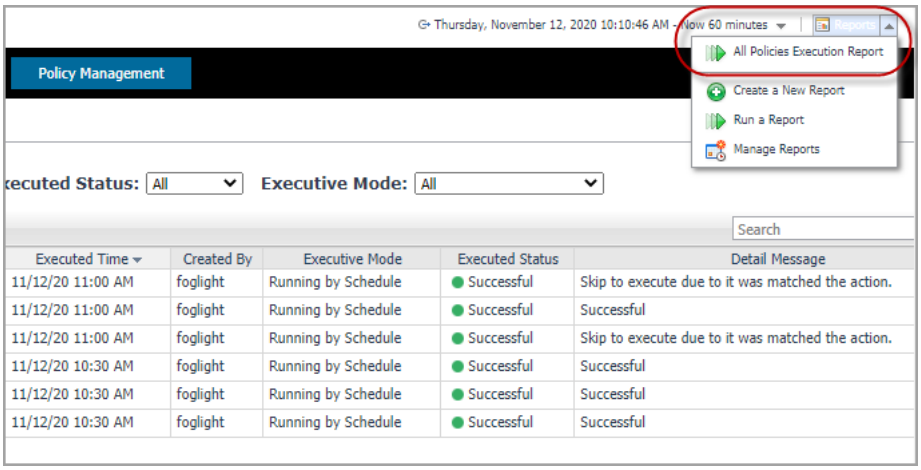


Run Reports for Policy Management

Click **Reports** on the top right corner of the interface and choose **All Polices Execution Report**. An *All Polices Execution Report* dialog box will appear. Fill in required information to run the report.

The *All Polices Execution Report* will summarize the status for all of the Policies Execution.

Figure 33. Run reports for Policy Management



About Us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit https://www.quest.com/.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.